WARSAW UNIVERSITY OF LIFE SCIENCES – SGGW
DEPARTMENT OF INFORMATICS

INFORMATION SYSTEMS IN MANAGEMENT XIV

Security and Effectiveness of ICT Systems

Scientific editors

Piotr Jałowiecki
Arkadiusz Orłowski

WULS Press Warsaw 2011

Warszawa 2011, I edition

Reviewers:

Prof. dr hab. Ryszard Budziński
Dr hab. Leszek Chmielewski, prof. SGGW
Prof. dr hab. Ludosław Drelichowski
Dr Urszula Grzybowska
Dr Andrzej Jakubiec
Dr inż. Piotr Jałowiecki
Dr hab. Maciej Janowicz, prof. SGGW
Dr Waldemar Karwowski
Dr Grzegorz Koszela
Dr Rafik Nafkha
Prof. dr hab. Marian Niedźwiedziński
Dr hab. Arkadiusz Orłowski, prof. SGGW
Dr Dariusz Strzęciwilk
Dr hab. Wiesław Szczesny, prof. SGGW
Dr hab. Antoni Wiliński, prof. ZUT
Dr Mirosław Woźniakowski
Dr Tomasz Woźniakowski
Dr Piotr Wrzeciono
Dr Tomasz Ząbkowski
Dr Andrzej Zembrzuski

Typesetting and prepress
Dr Piotr Łukasiewicz

ISBN 978-83-7583-371-3

Wydawnictwo SGGW

02-787 Warszawa, ul. Nowoursynowska 166
tel. 22 593 55 20 (-22, -25 – sprzedaż), fax 22 593 55 21
e-mail: wydawnictwo@sggw.pl, www.wydawnictwosggw.pl

Print: Agencja Reklamowo-Wydawnicza A. Grzegorczyk, www.grzeg.com.pl

PREFACE

Due to important and still increasing role of information in modern world there is a need for high level of stability, effectiveness, and security of ICT systems. The very important aspect of information management is an effective communication between various, often intensively cooperating, business institutions. This requires, among others, fast and secure data interchange.

Current monograph consists of 10 papers written by 20 authors coming from different institutions. It provides a rich source of ideas, concepts, solutions, and perspectives for nontrivial applications. We believe that presented results will be useful for all researchers, experts, and business practitioners, including managers themselves, which are dealing with different categories of information management systems. Chapters are ordered alphabetically, according to the surnames of the first-named authors.

Piotr Jałowiecki
Arkadiusz Orłowski

TABLE OF CONTENTS

HOW IT TOOLS SUPPORT BUSINESS PROCESS MANAGEMENT LIFE CYCLE STANDARDS: SURVEY OF STANDARDS AND MARKET OFFER

Beata Gontar, Agnieszka Grudzińska-Kuna, Anna Kaczorowska, Anna Pamuła, Joanna Papińska-Kacperek, Zbigniew Gontar

Department of Computer Science, Management Faculty, University of Łódź

Abstract. Business Process Management includes methods, standards and tools to support the design, enactment, management and analysis of operational business processes. Paper aims to review ongoing standards in the field and verify in what range chosen IT tools support them. The authors categorised relevant standards in relation to business process life cycle. Finally future developing trends of both standards and tools are presented. Findings of the paper are based on the literature review and analysis of selected software.

Keywords: business process management, standards, process life cycle, business process management systems, classification of standards

1. INTRODUCTION

Business Process Management (BPM) has attracted close attention in recent years due to its potential for increasing enterprise agility. Van der Aalst defines BPM as "*supporting business processes using methods, techniques and software to design, enact, control and analyze operational processes involving humans, organizations, applications, documents and other sources of information*" [1]. As the other areas of management, this one can be also supported by IT tools - Business Process Management System, that can automate, measure and improve business process (BP). Gartner uses another name - Business Process Management Suite (BPMS) and precisely defines its required capabilities. Thus BPMS must support modelling, monitoring, reporting and analysis of BP, support process change in the design and the execution (simulation and optimization), coordinate any type of interaction, and interoperate with external software assets. Interoperability BPMS with external application is often consider in relation to Service Oriented Architecture (SOA). Although SOA and BPM are two different disciplines, they share the common goals – increase in enterprise agility.

SOA represents a set of design principles that enable units of functionality to be provided and consumed as services [31]. Software application as a service has to

meet specific requirement. It has to be distributable and sharable, has clearly defined interface that specifies an explicit contract how it can be found and used [32]. Services are loosely coupled and vastly interoperable therefore they can be reused in many contexts.

Both researchers [33], [34] and software vendors [35] observed need for integration both disciplines in a short time. Many software leaders as IBM [35], Oracle [37], BEA [36], have put forward their own views how BPM and SOA can work together. Also some integrated BPM-SOA frameworks [34], [38] have been proposed by academia.

Services can be design to express business logic. They can encapsulate single task, sub-process or even entire process. Thus process model can be perceived as a specification of service components and human tasks that are orchestrated according to the business process logic. Threading together business services enables analysts to focus on real-time process adaptations, what seems to be important feature of modern BPM. New or changed process models with BPM tools can be implemented more rapidly because the SOA decouples the design process from the specific software implementation. Moreover classical workflow technology is embedded in SOA-style systems (cf. role of PBEL) [39] and modern workflow systems can incorporate services [40]. To sum up, BPM and SOA are counterparts. Their combination enables enterprise to be more agile and flexible in adopting the dynamic business context changes.

In 2006, according to the Gartner analysis, the BPMS market achieved almost $1.7 billion in total software revenue [26] and began to exhibit the characteristics of an early mainstream software market. Even in 2009, during the economic crisis, BPMS products had been continued to receive funding. Gartner estimated that the size of the BPMS market in 2009 totalled $1.9 billion in revenue [3].

The early BPM systems were made on demand, now software companies offer commercial, universal software applications, so a need for standards has appeared. This paper objective is to review BPM standards and verify in what range chosen IT tools support them. Before exploring BPM standards it is relevant to begin with an overview of BP life cycle.

2. BUSINESS PROCESS MANAGEMENT LIFE CYCLE

In general, management controls the use of resources and choreographs the operational activities of the enterprise. Management functions follow a life cycle of planning, organizing, staffing, directing, controlling and budgeting. BPM is the application of this management cycle to an organization's BPs [16].

There are many views of BPM life cycle, but following van der Aalst we describe four phases: (re)design and analysis, system configuration, enactment and monitoring, and diagnosis phase [10].

The process design phase is the identification of a new process or redesigning existing one. Here the process activities, their order, resource assignment and the organization structure are defined. Once the BP model is designed and verified, the configuration phase starts and the BP is being implemented. Next, the BP is performed by configuring the adequate information system. This system configuration phase may require important implementation efforts or may be a simple selection step. It depends on the underlying technology and on how much adjustment is needed. The BP model is enhanced with technical information that facilitates the enactment of the process by the BPMS. The system needs to be configured according to the organizational environment of the enterprise and the BPs whose enactment it should control. Then the process is executed and monitored in the process enactment and monitoring phase. One solution for processes automation is to develop/purchase an application that executes the necessary steps of the process. However, in practice, these systems seldom execute all the steps of the process exactly or completely [10]. Another approach is to use a combination of software and human intervention. This is more complex and makes the process documentation difficult. Business rules have been used by systems to provide definitions for governing behaviour, and a business rule engine can be used to guide process execution and resolution. Monitoring encompasses the tracking of individual processes, so that information on their state can be easily seen, and statistics on the performance of one or more processes can be provided. In this phase, data is collected for diagnosis phase. Here, the process is analyzed to find and identify the potential or actual bottlenecks and problems. The deployed process is examined and evaluated for improvement in next iteration of the BPM life cycle [17]. Diagnosis may be expanded to control and optimize running activity. Its outcome should be used as a feedback for the redesign the process model, in order to improve it and better suit to expectations and needs. Diagnosis of the actual process execution may result in its adaptation. These adjustments may involve some changes, which then may lead to a new or modified version of the BP for which the life-cycle starts again. Because of the automated support for managing the BP life-cycle, businesses can rapidly adapt to their ever-changing environment.

The business process life cycle's phases are supported by information technology standards. They allow the BP model to be portable and executable in almost any chosen hardware and software environment, eliminating the need to be tied to any specific vendor [15].

Ko et al. [9] submit BPM standards classification based on BPM life cycle and divide standards into four groups: graphical, execution, interchange and diagnosis. Graphical standards allow users to express in graphical way behavioural, functional, organizational and informational features of BPs. Execution standards computerize the deployment and automation of BP. Diagnosis standards are intended to facilitate emergence of specialized products that can help to analyze

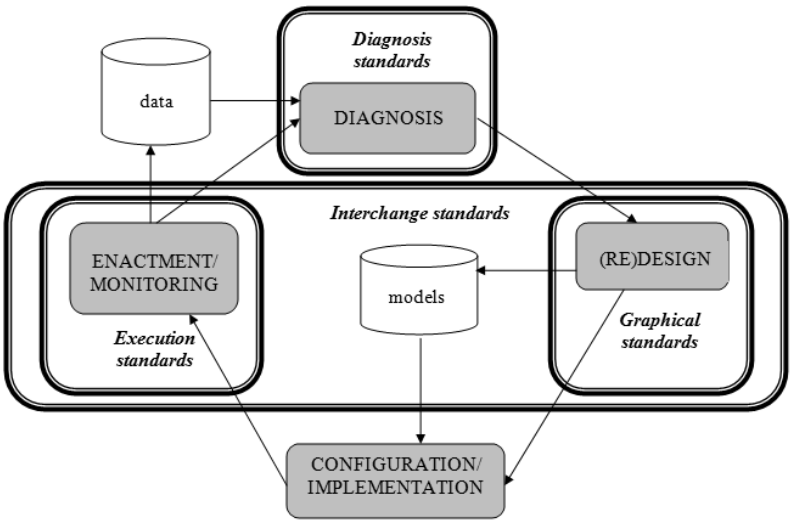

Figure 1. Standards support for BPM life cycle.
Source: own preparation based on [1]

BP in real time. Exchange standards are used to transfer different BP definitions among various BP applications. The short description of chosen standards is presented below.

3. GRAPHICAL STANDARDS

The increasing interest in business process modelling has resulted in the appearance of various Business Process Modeling Languages (BPMLs) that allow users to express in graphical way behavioural, functional, organizational and informational characteristics of business processes. Among usually mentioned graphical notations there are: Business Process Model and Notation (BPMN), Event Process Chains (EPCs), Unified Modeling Language 2.0 Activity Diagram (UML 2.0 AD) and Integrated Definition Method 3 (IDEF3).

This article focuses on BPMN and UML 2.0 AD as the standards that are currently the most expressive and the easiest for integration with the interchange and execution level [9].

Business Process Model and Notation. It was in 2001 when Business Process Management Initiative began developing Business Process Modeling Language. They soon realized that there was a need for graphical representation. Required notation was to be accessible to all business users and to provide facilities to translate models into an executable form. In 2004 the Business Process Modeling Notation (BPMN) 1.0 specification was released to the public. In 2006 that specification was

adopted as an OMG standard (after the merger of BPMI.org and OMG) [30]. Consecutive two versions 1.1 (2008) and 1.2 (2009) included only minor updates

BPMN 2.0 released in 2010 is "stable and mature" version with significant changes compared to the previous ones. BPMN now stands for business process model and notation because OMG wanted to call attention to the standard's XML aspects [23].

Primary goal of BPMN remains the same: readability, flexibility and expandability. BPMN as a next generation notation is to facilitate the understanding of business processes performance and communication of all business users involved in process life cycle. Business process's complexity can be modelled by elements such as activities, events, gateways, flows, swim lanes etc., that are compliant with most flow-charting notations. BPMN offers also advanced modelling concepts like exception handling, transactions and compensation. Version 2.0 formalizes execution semantics for all BPMN elements. Notably, BPMN is able to handle three types of submodels within end-to-end business process: private and public processes (orchestration), choreographies and collaborations. The latest version incorporates model of choreography to take into account that e-commerce processes are choreography-based rather than conversation – based or orchestration-based [23].

Another BPMN 2.0 goal is to enable portability of process definitions. The specification contains the meta-model and schema for BPMN 2.0 Diagram Interchange (BPMN DI). The BPMN DI meta-model is defined as a MOF-based meta-model and by an XML schema as well. Moreover BPMN 2.0 can be mapped to XML languages designed for the execution of business processes such as WSBPEL (Web Services Business Process Execution Language). Mapping of subset of BPMN to WS-BPEL 2.0 is included in the specification [18].

The theoretical underpinnings of BPMN are largely based on Petri nets. Originated from Petri nets concept of token is employed to define the behaviour of a process that is being performed [22].

UML 2.0 Activity Diagrams. The Unified Modeling Language (UML) is most-used OMG's specification. It is a graphical language for visualizing, specifying, constructing, and documenting the artefacts of distributed object systems [18].

UML has been developing by OMG since 2000. Although the latest version (2.4 Beta 2) was released in March 2011 significant changes were introduced by version 2.0 (2005). Since then UML has included 13 distinct types of diagrams capturing detailed design models of software systems. These models provide foundation for translation into some enactment technology (usually program code) either by developers or in semi-automated manner via CASE tools [20]. As diagrams differ in level of abstraction and modelling perspective, UML can be tailored for several purposes. Particularly Activity Diagrams (AD) can be used for business process modelling. The UML AD is both flowcharting technique and a special kind of state machine (based on Harel's statecharts). Like BPMN, UML AD is rooted in Petri net

token semantics. Graphically AD is composed of nodes and edges. Nodes represent actions, activities, data object and control nodes. Edges depict flow of control. Action is fundamental, atomic unit of behaviour. The language provides detailed action taxonomy (40 different types) and several types of control nodes. Activities consist of actions and/or other activities.

In literature, suitability of UML 2.0 AD as BP modelling technique is assessed mainly on the bases of Workflow Patterns [20], [19]. Russell's evaluation indicates that whilst UML 2.0 ADs have its merits, they are not suitable for all aspects of BP modelling. They offer sufficient support for control-flow and data perspective, but they are extremely limited in modelling of resource-related and organizational aspects of business processes.

To conclude, graphical notations being foundation of modelling enable business process to move through its lifecycle. Although developers of graphical standards pay a close attention to their legibility and accessibility to all business users, authors' academic experience and some empirical researches [22] suggest that their applying requires intensive training and education as the cost of fixing errors made in conceptual specification (due to lack of expertise in process modelling) are very high [40].

Development of both analyzed notations lies in resolving inconsistencies and ambiguities of privies versions and formalization of their elements execution semantics [21].

4. EXECUTION STANDARDS

Ko Ryan K.L. et all in their BPM standards classification proposal define execution standards as those, which allow to computerize the deployment and automation of business processes, and referring to the BPM life cycle model, they conclude, that execution standards dominate the stage of process enactment [9].

There are currently three prominent execution standards, all of them described as standards for Web Service composition: Business Process Modeling Language (BPML), Business Process Execution Language (BPEL), and Yet Another Workflow Language (YAWL).

BPML is a vendor driven standard, developed by BPMI.org, with prominent involvement of Intalio Inc. It was commercially deployed in early-stage BPMS. BPMI.org released the following versions of BPML: BPML 0.4 (submitted to BPMI members in August, 2000, and public released in March, 2001), and BPML 1.0 (June, 2002). BPML has not been supported by BPMI.org, since its merger with OMG. BPML (BPMI.org), and BPEL4WS (Microsoft, IBM, et al.) have been submitted to OASIS, and this standardisation organization has created a Business Process Execution language standard called Web Services – Business Process Execution Language (WS-BPEL).

BPML's current status is that it is serving – as being formally complete – as a benchmark for the comparison of BPEL's features for the WS-BPEL committee [29], [12].

BPML is a XML-based declarative language, which provides a formal model for expressing executable processes [28]. The features of BPML are as follows: end-to-end process modelling, control-flow/data-flow separation, produce/consume messaging, dynamic control flow, transparent persistence, embedded business rules, nested processes, distributed transactions, process-oriented exception handling, and pi-calculus as underlying mathematical model.

BPEL is another vendors driven standard, developed initially as Business Process Execution Language for Web Services (BPEL4WS) by standard consortium consisting of BEA Systems, IBM, and Microsoft. The consortium made available specification BPEL4WS 1.0 in June, 2002, as combined ideas from Microsoft's XLANG, and IBM's Web Services Flow Language (WSFL). In May, 2003 revised proposal, with additional contributions from SAP, and Siebel was submitted, as BPEL4WS 1.1 specification, for the standardization to OASIS standardisation consortium, resulting in 2004 as WS-BPEL 2.0 (in short: BPEL). BPEL has been commercially deployed in numbers of BPMS, currently having position of dominance on the BPMS market.

BPEL is a XML-based meta-language, which in an abstract view, describes in SOA how a company performs its BPs (represented by Web services). In this sense, it could be described as a Recursive Aggregation Model for Web Services, enabling composition, orchestration, and coordination of Web services [11]. On the level of Process Usage Patterns, BPEL defines executable processes (which contain the partner's business logic behind an external protocol), and abstract processes (which define the publicly visible behaviour of some or all of the services an executable process offers, and define a process template embodying domain-specific best practices) [13].

BPEL constructs encompass: process definition, recursive composition and partner links, variables, variable properties, correlation sets, basic and structured activities, scopes, and compensation handling [13], [14].

YAWL is a state-of-the art, academic driven standard, developed by research group from TU Eindhoven and Queensland University of Technology, and deployed in open source YAWL system, available under the LGPL license, and used mainly for teaching at the universities [10].

As Hofstede et al. have observed, vendor driven standardization bodies efforts have essentially failed, resulting in a lack of widespread use of BPM technology [10]. They have stated, that a lot of shortcomings and limitations of commercial standards led to the emergence of the new BPM environment - YAWL, based on the workflow patterns, providing control flow patterns support, and having formal foundation in set theory, predicate logic (syntax) and Petri net (semantics).

YAWL does not give the process model prescription, but – instead – guide to process's objective through the catalogue of possible actions, choices to be made dynamically from the catalogue of workflow patterns at the runtime by considering context of specific instance of the process, and dynamically extension of the catalogue at the runtime [10].

5. INTERCHANGE STANDARDS

BPM life cycle phases rarely are realized by using one particular software. Usually modelling is done by one application while further analysis and implementations by other packages delivered by different vendors. For the proper way of saving and exporting BPMN models interchange standards are necessary. Two ideas: XPDL and BPDM will be shortly introduced here.

Business Process Definition Metamodel (BPDM) is a standard definition of concepts that allow expressing BP models as the metamodels. The standard was issued by OMG in 2003, adopted in initial form in July 2007 and finalized in July 2008. Metamodels define concepts, relationship, and semantics for exchange BP specifications between different modelling tools, and further between these tools and execution environment due to XML for Metadata Interchange – XMI. It is important, that only necessary elements are seen by users of different tools.

Business Process Modeling Notation standard did not have metamodel and it only appears in Business Process Model and Notation 2.0. Earlier metamodels were only in BPDM.

XML schema (XSD) and XMI are defined as exchange formats for OMG's metamodels transformation to XML.

Two joint specifications: Business Semantic for Business Rules (BSBR) and BPDM were created by OMG for better accommodation of business process modeling. BPDM simplify the usage of activity models in UML 2.0 and define connections with process and its automation, organization and its strategy. So, the field of BPDM is not only business process automation analysis but value chain and organization analysis as well.

Owing to a common abstract metamodel BPDM provides that models created in different specialized concepts will be interpreted in the same way while being moved to a different tool. Thus metamodel standardizes software access to definitions of processes, enables access to reusable libraries of these definitions and supports for integrating rules within processes. Moreover BPDM acts as translator between various notations, using BPMN as standard notation for processes.

OMG defines metamodels in MetaObject Facility language. "*BPDM relies on a formal method - PSL (Process Specification Language) - a first order logic language to ensure execution consistency of processes*" [18].

Definitions of processes can be modeled in BPDM not only on the level of orchestration but also choreography. Orchestration defines process activities within one organization. Choreography models the way how independent parties communicate in business process. BPDM has also the ability to reconcile the choreography with supporting internal business processes.

XML Process Description Language (XPDL) is a standard defined and approved by Workflow Management Coalition (WfMC). It provides a file format that supports every aspect of the BPMN process definition notation including graphical descriptions of the diagram, as well as executable properties used at run time XPDL v 1.0 was released in 2001. In 2002 beta version of XPDL was released together with a supporting XML schema describing the meta-model. The WfMC's Interface One (one of five functional interfaces of a workflow service identified by the WfMC as a part of its standardization program) was a general base for those documents [42]. Current version is XPDL v 2.1 and it is capable of handling BPMN 1.1 constructs. According to Shapiro and Gagne from WfMC forthcoming XPDL v 2.2 is covering only a subset of the process modelling conformance class of the BPMN 2.0 specification. The XPDL 2.2 schema is completed and has been validated and tested with Specification Document initiated. The XPDL 3.0 is expected to focus on covering the complete BPMN 2.0 specification and schema. Works are going on now and XPDL 3.0 schema covering all visual elements has been completed and validated, non visual attributes inclusion has started but is not completed and unfortunately XPDL 3.0 Specification Document has not been started [24].

XPDL was design to enable the data compatibility between modelling tools and different BPM engines; moreover it is supposed to allow for the interchange between modelling tools and simulation tools or optimization tools. The design interchange is possible due to implementation of an idea of one-for-one representation of the original BPMN process diagram and ‘XY' (or vector) coordinates, including lines and points that define process flows. The solution allows for process to be written and re-read to recover the original diagram. As J. Pyke concludes: “*For this reason, XPDL is effectively the file format or "serialization" of BPMN, as well as any non-BPMN design method or process model that use in their underlying definition the XPDL meta-model*”[41].

It must be noticed that XPDL is not an executable programming language but process design XML format for storing process syntax for BP models and graphical information of the process elements. XPDL is particularly suitable for implementation of file format exchange of BPMN diagrams. It includes concepts like: task input/output, control flow, data handling, human interactions as a part of a business process e.g. roles, events and exceptions.

The process language does not define exact execution semantics for the different activities like BPEL and is technology neutral.

Both BPDM and XPDL can exchange BP definitions by BP tools. OMG aims to reconcile BPMN and BPDM into a consistent language. Future implementations of BPDM will provide support for BPMN and translation to XPDL. The maturity of the XPDL can be defined as well-adopted interchange standard that in successive releases follows graphical and execution standards. As a stable for a long time standard XPDL was widely accepted and adopted by the open source community. An important factor of its wide deployment is that XPDL is made freely available without any licensing restrictions. The number of vendor supporting XPDL is instantly growing. In Gartner's BPMS Magic Quadrant list published in 2006, eight of the best eleven vendors claimed to support XPDL. On the WfMC list about 80 products implementing XPDL is presented now, however only some of them support XPDL 2.x.

6. DIAGNOSIS STANDARDS

The diagnosis phase is realised by Business Activity Monitoring (BAM) - a unit of BPMS, which use data stored in the previous phase to diagnosis. Therefore its tasks are: aggregation, analysis and presentation of real-time information about the process.

BAM specifically focuses on critical business indicators like key performance indicators (KPIs) [5]. BAM aggregates business events e.g. customer orders and inventory updates to transform them into rules to generate alerts. Very useful technique for task analyzing is process mining, i.e. extracting process models (so extracting knowledge) from event logs. It can be considered as a special case of data mining. The first step is gathering information about the process that has been executed i.e. about the sequence of the events taken place. The next task is creating a process specification, which properly models the registered behaviour.

BAM solution can collect data from many sources, not only from BPM System. In the past a similar idea appeared in workflow systems. In 1996 a format CWAD (Common Workflow Audit Data) was created - for standardisation process audit events. It allows for using data from different sources i.e. different workflow systems. This standard has never found acceptance in commercial systems, because it was not based on XML which was under development then. Today a similar idea is proposed - BPAF Business Process Analytics Format [27].

Usually BAM tools make a dashboard for users to allow them observing the processes progress, performing analysis and viewing custom reports. Common reporting tools can be used to process BAM data. The user can obtain report by making SQL queries or use dedicated tool. Techniques are evolving from XQuery, SQL and attempts in applying stream processing to the semantic methods. In publications two standards of diagnosis phase are the most commonly reported: BPQL and BPRI, with

remark that they are immature or unfinished. Up till now their specifications has not been published.

Business Process Runtime Interfaces (BPRI) is a platform-independent model (PIM) of the runtime interfaces to BP engine. It describes instances of processes and their activities like current state, current variable values [2], [6]. BPRI allows for administration and monitoring. The initiative was established in 2002 by OMG. The specification would have been completed by the end of 2007, but it has not been released to the public till now.

Business Process Query Language (BPQL) is a flexible object-oriented query language derived from Stack-Based Query Language. BPQL has clear syntax and unambiguous semantic [7] BPQL enables monitoring of BPEL process code and can be integrated with XPDL. BPQL was initiated in 2002 by BPMI, and probably has been on hold after the merger of OMG and BMI.

In publications we can find other concepts like Bpath [8] or BQL [4]. It is difficult to say if any of them will become a real standard.

The multiplicity of proposed solutions can provide a weight of problem diagnosis. This phase distinguishes BPMS from the previous initiatives, so maybe the standard development process needs much more time. Creation of applications based on SOA creates possibility to use only basis and proven standards like XML or SQL.

7. APPLICATION COMPARISON – A MARKET SURVEY

A survey through the market offer has been conducted to find out how market tools support described standards. For each of the BPM phase a grate number of supporting applications (commercial and open source) exist. To shorten the list, the

Table 1. Comparison of tools delivered by vendors selected in PROCESOWCY.PL report.

Software	Graphical		Interchange		Execution	Diagnosis	
	BPMN	UML	XPDL	BPDM	BPEL	BPRI	BPQL
ADONIS	Y	Y	Y		Y		
ARIS	Y	Y	Y		Y		
BONAPART®		Y	Y		Y		
iGrafx	Y	Y	Y		Y		
K2 blackpearl	Y						
Metastorm	Y	Y	Y		Y		
OfficeObject® WorkFlow	Y	Y	Y				Y
Piramid WorkFlow	Y						
Visio	Y	Y	Y*		Y*		
WebSphere Lombardi Edition	Y			Y	Y		
* - Via additional tool							

Table 2. Comparison of tools supplied by vendors reported in Magic Quadrant.

Software	Graphical		Interchange		Execution	Diagnosis	
	BPMN	UML	XPDL	BPDM	BPEL	BPRI	BPQL
ActiveVOS	Y		Y		Y		
Adobe LiveCycle Enterprise Suite	Y		Y		Y		
AgilePoint BPMS			Y		Y		
Appian Enterprise	Y				Y		
BizAgi	Y		Y				
Cordys Business Operations Platform			Y				
EMC Documentum xCelerated Composition Platform	Y		Y		Y		
Fujitsu Interstage BPM	Y		Y				
Global 360	Y		Y				
BizFlow BPM Suite	Y				Y		
FileNet Business Process Manager			Y		Y		
IBM WebSphere Lombardi Edition IBM BPM Blueprint	Y		Y	Y	Y		
IBM WebSphere Dynamic Process Edition (replaced by IBM BP Manager)	Y		Y		Y		
Intalio/BPMS Enterprise Edition	Y				Y		
K2 blackpearl					Y		
Metastorm BPM	Y	Y	Y		Y		
OmniFlow					Y		
Oracle BPM Suite	Y		Y		Y		
BPMone	Y						
PRPC	Y				Y		
Sequence BPM Suite,					Y		
Polymita Business Suite					Y		
Savvion BusinessManager	Y		Y				
SAP NetWeaver BPM SAP NetWeaver Business Rules Management	Y						
Singularity Process Platform							
Software AG's webMethods	Y		Y				
Tibco iProcess Suite	Y		Y		Y		

survey has been limited to software evaluated in report prepared by team of Polish portal PROCESOWCY.PL in January 2011 [25] (Table 1 presents the result) and

BPMS evaluated by Gartner Magic Quadrant in October 2010 [3] (Table 2 presents the result).

It should be mentioned that in some cases, versions later than pointed out in reports were examined because of appropriate data availability.

Although the software coming from international and Polish market is not exactly the same, both tables present similar results - the same groups of standards as the most often implemented. Functionality and complexity of the software also determines number of supported standards. BPMS e.g. IBM WebSphere Lombardi Edition supports more than one standard for interchange phase. BPMN, XPDL and BPEL seems to be widely accepted standard. BPRI and BPQL were promising potential standards but being still uncompleted they cannot be implemented in commercial tools. Research should be continued after their release to find a leader for the diagnosis phase.

Adoption of given standard can have different meanings. Software can be based natively on the standard (e.g. BPEL) or can export or import files in suitable format (cf. Oracle BPEL Process Manager). Moreover application can use standard notation (e.g. BPMN) or use its own notation that is semantically compliant with it.

UML 2.0 AD has its merits as BP modelling tool, but UML itself comes from object-oriented software engineering therefore only tools that have wide scope of deployment like Visio or Aris use it.

Some application allows only for import or export of specified format, in some cases additional software is required to ensure compliance with particular standard.

Undoubtedly there are a lot of BPMS that do not support any standard; however our survey shows that BPMS market leaders widely adopt the most prominent standards.

8. SUMMARY AND CONCLUSION

Generally speaking, technical standards increase interoperability and compatibility of software applications. Sometimes they are the best solution to vendors lock-in. They also ensure desirable characteristics of subject they address. In the BPM context, standards enable portability of process definitions between different BPM life cycle phases or between tools delivered by different vendors. On the other hand they can limit their users in expressing complexity of real-life BPs.

In past ten years there were many standardization initiatives, some of them reached their maturity whereas the others did not stand the test of time or lost favour with practitioners.

Although developers of graphical standards pay a close attention to their legibility and accessibility to all business users, authors' academic experience and some empirical researches suggest that their applying requires intensive training and education. Development of both analyzed notations lies in resolving inconsistencies and

ambiguities of previous versions and formalization of their elements execution semantics. Nevertheless, the industry is currently consolidating towards BPMN as graphical standard.

XPDL and BPDM serve as an interchange mechanism in a quite different way. In our survey only a few software tools use BPDM, whereas XPDL is more widely adopted. Although the maturity of the XPDL can be defined as well-adopted, it is still chasing the graphical and execution standards trends.

Comparing BPML to BPEL shows that both share similar roots in Web services and leverage other Web services specifications, however, BPML supports modelling more complex business processes, therefore it can be regarded as a superset of BPEL. Because BPEL is not formally complete it need some extensions to compensate for its deficiencies e.g. BPEL4People – for human involvement, BPEL Subprocesses – for treating invoking services as another processes, BPELJ – for allowing inline Java code in BPEL process.

In fact, there is still need for standardization of the diagnosis phase of BPM life cycle. Both BPRI and BPQL have not been completed yet. Diagnosis phase is the youngest part of BPM life cycle and therefore maybe it need more time to establish appropriate standards. On the other hand, for BAM modules provided by most of BPMS vendors, SQL and XML can be sufficient so there is no industry's push for standards at the moment.

REFERENCES

[1] van der Aalst W. M. P., ter Hofstede A. H. M., Weske M., (2003) *Business process management: A survey*, in Proceedings of the Business Process Management: International Conference.

[2] Havey M., (2005) *Esential Business Process Modeling*, O'Reilly Media.

[3] Hill J. B., Sinur J., (2010) *Magic Quadrant for Business Process Management Suites*, Gartner Research.

[4] Jin H., Wang J., Wen L., (2011) *Querying business process models based on semantics* DASFAA'11 Proceedings of the 16th international conference on Database systems for advanced applications: Part II, Springer-Verlag.

[5] Lubiński T., (2008) *Business Activity Monitoring: Process Control For the Enterprise*, http://www.sl.com

[6] Miers D., (2007) *The OMG Business Process Related Standards, An emerging set of standards that enable Model Driven businesses*, BPM Focus.

[7] Momotko M., Subieta K., (2004) *Process Query Language : A Way to Make Workflow Processes More Flexible* in Advances in Databases and Information Systems Springer.

[8] Sebahi S., Hacid M., (2010) *Business Process Monitoring with Bpath*, International Conference on Cooperative Information Systems CoopIS, Springer.

[9] Ko R. K. L., Lee S. S.G., Lee E. W., (2009) *Business process management (BPM) standards: a survey,* Business Process Management Journal, Vol. 15, No. 5.

[10] ter Hofstede A. H. M., van der Aalst W. M. P., Adams M., Russell N., ed., (2010) *Modern Business Process Automation. YAWL and its Support Environment*. Springer, Heidelberg, Dordrecht, London, New York.

[11] Juric M. B., Chandrasekaran S., Frece A., Hertis M., Srdic G., (2010) *WS-BPEL 2.0 for SOA Composite Applications with IBM WebSphere 7. De-fine, model, implement, and monitor real-world BPEL 2.0 business processes with SOA-powered BPM*. Packt Publishing.

[12] Weske M., (2007) *Business Process Management. Concepts, Languages, Architectures*. Springer-Verlag Berlin Heidelberg.

[13] König D., (2009) *Web Service Orchestration and WS-BPEL 2.0*. SFM-09WS – 9th International School on Formal Methods for the Design of Computer, Communication and Software Systems – Web Services – June 1-6, 2009 – Bertinoro.

[14] OASIS, (2010) *Web Services Business Process Execution Language (WSBPEL),* http://www.oasis-open.org

[15] Madsen M., (2006) *Unlocking the Power of SOA with Business Process Modeling*, CGI Group Inc.

[16] zur Muehlen M., Ting-Yi Ho D., (2006) *Risk Management in the BPM Lifecycle*, Business Process Management Workshops - BPM 2005 International Workshops, Springer, Lecture Notes in Computer Science, Volume 3812/2006.

[17] Recker J., Mendling J., (2006) *On the Translation between BPMN and BPEL: Conceptual Mismatch between Process Modeling Languages*, Proceedings 18th International Conference on Advanced Information Systems Engineering. Proceedings of Workshops and Doctoral Consortiums.

[18] OMG, (2011) http://www.omg.org/spec/

[19] Wohed P. et al., (2006) *On the Suitability of BPMN for Business Process Modelling,* in Proceedings 4th International Conference on Business Process Management 4102, Vienna, Austria. Copyright Springer.

[20] Russell N. et al., (2006) *On the Suitability of UML 2.0 Activity Diagrams for Business Process Modelling,* in: Research and Practice in Information Technology, Vol. 53, Australian Computer Society, Inc.

[21] Peixoto D. C. C. et al., (2008) *A Comparison of BPMN and UML 2.0 Activity Diagrams*, accessed from http://homepages.dcc.ufmg.br/~cascini/SBQS_2008.pdf

[22] Recker J.C., (2010) *Opportunities and Constrains: the Current Struggle with BPMN*, BPM Journal, 16(1), Emerald.

[23] Earls A., (2011) *The rise and rise of BPMN for process modeling, BPMN 2.0: The emerging star of business process*, accessed from http://www.ebizq.net

[24] Workflow Coalition, (2011) http://www.wfmc.org

[25] *Porównanie narzędzi wspierających BPM,* (2011) http://www.procesowcy.pl

[26] Hill, J. B., Cantara, M., Deitert, E., and Kerremans, M. (2007) *Magic Quadrant for Business Process Management Suites,* Gartner Research.

[27] zur Muehlen M., Swenson K.D. (2011) *BPAF: A Standard for the Interchange of Process Analytics Data,* In Business Process Management Workshops'2010. Springer.

[28] Shapiro R., (2002) *A Comparison of XPDL, BPML and BPEL4WS.* Cape Visions.

[29] Owen M., Raj Jog, (2003) *BPMN and Business Process Management Introduction to the New Business Process Modeling Standard,* Popkin Software.

[30] White S. A., (2008) *BPMN Modeling and Reference Guide: Understanding and Using BPMN*, Future Strategies.

[31] Lankhorst M. et. al. (2009) *Enterprise Architecture at Work,* Springer-Verlag, Berlin Heidelberg.

[32] Abrams Ch,. Schulte R. W., (2008) *Service-Oriented Architecture Overview and Guide to SOA Research*, Gartner Research, ID Number G00154463.

[33] Malinverno P., Hill J. B., (2007) *SOA and BPM Are Better Together*, Gartner Research, ID Number G00145586.

[34] Nan Wang, Lee V., (2011) *An Integrated BPM-SOA Framework for Agile Enterprises* in N.T. Nguyen, C.-G. Kim, and A. Janiak (Eds.): ACIIDS 2011, LNAI 6591,. Springer-Verlag Berlin Heidelberg.

[35] Noel J., (2005) *BPM and SOA: Better Together*, IBM White Paper.

[36] Percival M., *BPM and SOA: Putting SOA to work with BPM* , www.eudownload.bea.com/uk/events/bpm /Edinburgh/BPM-and-SOA.pdf

[37] McGlauchlin Ph., *ORACLE-Business Process Analysis Suit: Overview & Statement of Direction*, http://www.oracle.com

[38] Bajwa, I .S., et al., (2008) *SOA and BPM Partnership: A paradigm for Dynamic and Flexible Process and I.T. Management*. World Academy of Science, Engineering and Technology.

[39] van der Aalst W .M. P., et al. (2009) *Flexibility as a Service*, DASFAA 2009 Workshops in Chen L. et al. (Eds.):, LNCS 5667, Springer-Verlag Berlin Heidelberg.

[40] Brahe S. (2007), *BPM on Top of SOA: Experiences from the Financial Industry*,. Alonso G., Dadam P., and Rosemann M.,(Eds.) BPM, LNCS 4714, Springer-Verlag Berlin Heidelberg.

[41] Pyke J., (2010) *XPDL - The Silent Workhorse of BPM,* http://www.bpm.com/xpdl-the-silent-workhorse-of-bpm.html

[42] Cover R., (2004) *XML-Based Workflow and Process Management Standards: XPDL, Wf-XML,* http://xml.coverpages.org/wf-xml.html

ASSESSMENT OF THE USEFULNESS OF INTEGRATED MANAGEMENT SYSTEMS

Magdalena Graczyk

Department of Engineering Management, Poznan University of Technology

Abstract. In the current Information Era access to quality information characterized by appropriate levels of usefulness and short search time becomes an extremely important criterion in the competition not only between companies but also between countries. Based on characteristics of the integrated information systems, features of information and areas such as: infonomics, economics of information, management, quality management, and marketing, presents a model assessing the usefulness of integrated management systems. The concept of utility is described by a number of features, where each of them has an index describing its compliance or not. Criteria for the validity of the characteristics specified by the user and meets the critical indicators of the system demonstrates the usefulness of integrated management systems. The integrated system must meet the information needs of user group, only in this case will fulfill its role of utility.

Keywords: integrated management systems, information access supporting systems, utility, quality, information, characteristics of information

1. INTRODUCTION

Rapid development of information and communication technologies in the last century has influenced immensely not only the functioning of enterprises but also the entire society [1]. Building the information society is a priority of every developing country. The notion of information society is defined in a document e-Poland – Strategy of information society development in Poland in years 2001-2006 as "Information society - a new society system shaping in countries with high level of technological development, where information management, its quality and conveyance speed are a key factor of competitiveness, both in industry and services, and the development level requires using new ways of gathering processing, conveying and using information" [2]. The development of information technology has moved the possibility of acquiring and gathering information beyond the perception of one man. Pertinent user information is stored most in data bases. These data often are copied to the system with existing databases. Making such decisions is associated with high risks related to data errors [3]. It is harder

and harder to find current, reliable and public information in time acceptable for its recipient. The Internet has caused that currently the society members have access to many information datasets (excess of information) impossible to be processed individually [4]. An increasing amount of searched information, including that from Internet, does not fulfill the basic criterion of pertinence. Such situation is a result of misunderstanding the informational needs of users, dispersed data and lack of current and reliable information digitalized in a form enabling combining the databases with integrated information systems. It is also connected with relevance and redundancy, as well as shortening the time between information need occurrence and making decision about the necessity to acquire that information [5]. Information in digitalized form are stored in data bases, which are the core of many IT systems created for various social groups and organizations. Only effective, reliable data bases, containing current and solid data guarantee efficient functioning of a system, understood as a set of interconnected elements isolated from the environment. Information system makes it possible to acquire and transform information, which results in certain decisions [6]. It's worth reminding, that when making a decision a user goes through two phases composed of several stages each. First phase engages information systems the most and consists of the following actions:

- „recognizing and describing the problem that requires making a decision, including determining the range of the problem, areas of activity it relates to and competent people in the subject the problem concerns;
- collecting information about the problem and methods of solving it;
- determining circumstances that must be considered so that the solution would be correct;
- collecting opinions of experts;
- preparing a diagnosis of a situation that would consist evaluation of economical, technical and organizational possibilities of solbing the problem;
- shaping alternative solutions for the analyzed problem that would be considered as acceptable for the company" [7] and people.

The figure1illustrates the course of the first phase, in which the management supporting systems play an important role. Second phase is a decision making process, formulation of models and performance of models and performance of a simulation, cognition of the other opinions and solutions [8].

The article discusses the issues of information systems in management, designed for a widely understood community and economic entities.

Defining the needs of future information systems users as well as the properly conducted process of a system designing, [9] testing and implementation, is a crucial activity in designing the useful information systems. Information, in order to serve its purpose, should be defined by characteristics which describe it, as well

a defined criterion of usefulness described by indexes allowing to assess the utility of a given system.

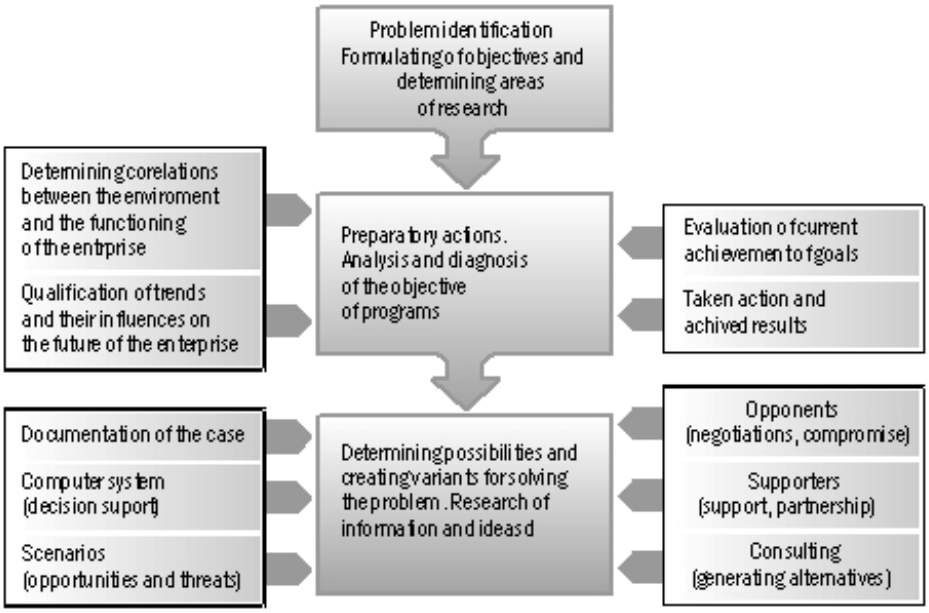

Figure 1. Preparation of cesisive proces. Source: E. Więcek-Janka, Games and Decisions, Wyd. Politechniki Poznańskiej, Poznań 2011, op. cit. p. 24

2. INFORMATION IN SOCIAL AND ECONOMIC SYSTEMS

Information is currently the most valuable component of created innovative solutions, and new information technologies accompany humans in all areas of everyday life. In times of development of modern information technologies, new scientific disciplines emerge, combining IT and economy (particularly management). Such scientific disciplines as economic informatics support the information flow in organizations [10]. In times of development of modern technologies, IT systems are more and more often used by city dwellers or tourists. The examples of such systems are local systems, helping in acquiring information about accommodation, gastronomy or touristic objects. Systems [11] which use particular information technologies should fulfill the pertinence criterion, and the processes related to delivering information should be flexible enough to be adjustable to changing environment and users' needs. Dispersion of data makes it impossible to find suitable information in a short time, however new information

technologies with a use of media convergence allow for merging of information and creation of integrated information systems [12]. Information system is described in management as an “entirety of formal and informal sets of information, points of generating, distribution channels and points of gathering and processing information" [13]. „The objective of information system is to deliver to receivers-decision makers useful information needed to make decisions. A decision maker bases his decision on information he has.” [14] In present times, the development direction of information systems is not only the entrepreneurs activity but also a necessity to deliver the processed information to the society. Such systems allow for quicker and more apt decision making and minimization of information noise.

Under social and economic information system we should understand:

- all sets of information, where each of them is pertinent for at least one system user, which come from sources in which data is gathered and shared by public institutions, private institutions and information brokering entities.
- relationships between public institutions, private institutions and other information brokering entities, which distinguished their own organizational or social culture,
- system users, subjects creating this system, who have their own needs (defined by information characteristics) and want to satisfy them with a use of the systems,
- set of relationships between particular sets, which created the system

It is also worth noticing, that public and private institutions as well as individual entities and other subjects are characterized by diversified organizational and social culture. Problems with preparing a proper message are mainly based on the cultural differences, which, because of views, beliefs or language, sometimes make the recipient incapable of decoding the message[15]. Influence of the culture may thus be crucial in semantic noise of transferred information. The culture itself consists of multiple factors, such as norms, ideas, symbols, learned reactions, attitudes, beliefs, traditions, etc. Therefore this notion relates to certain attitudes and behavior. In regard to information systems, we may talk about certain traits of subjects, which may influence the pertinence of data, for example a frequency of updates or willingness to share the data. The wider the area of system functioning is the more important is the culture of a given individual.

In social and economic systems we encounter functional specialization of information processes, where this specialization according to J. Oleński can be done in one or several functions [16]. Integrated systems are no longer based only on primary information but are more and more often supported with secondary information, selected based on the evaluation of information quality and their characteristics. „Nowadays, economy market requires to apply a new methods of management to gain the economic goals. To achieve this goal it is necessary to manage the information to join marketing with quality. Such a functions can be

realized by CRM FQ *(Customer Relationship Management for Quality)* system which determines the connection CRM *(Customer Relationship Management)* system with QFD (*Quality Function Deployment)*."[17] Social and economic information systems will also be based on decision support systems, helping the users to find pertinent information and to properly evaluate the usefulness of information acquired from the information system. One of the first supporters of usability – Jakob Nielsen – describes 5 of its most important elements.

1. Learnability – how easily can the users perform elementary tasks during first contact with a service?
2. Efficiency – how quickly are the tasks performed by a user already familiar with a service?
3. Memorability – how quickly can a user achieve proficiency in using the service after a long absence?
4. Errors – how many errors are made by users, how are they communicated and how quickly and in what ways will the users be able to deal with these errors?
5. Satisfaction – do they users like using the service?[18]

Decision supporting systems (DSS) represent an approach based on a usage of computers and information to make managerial decisions [19] and more and more often also the decision regarding entire society. DSS facilitates decision making processes, focuses attention on supporting and not automating the decision, is capable of reacting equally quickly to the changes of system users' needs [20]. Based on a definition of an information system integrating the databases belonging to various users to one decision supporting system, we may distinguish a set of elements:

$$ISISS = \{G, B, T, D, I, U, M, D, R\} \quad (1)$$

where:
ISISS – information system having symptoms of integrated supporting system,
G – groups of users, and their abilities to adopt innovative solutions in the area of information systems,
B – data bases, which contain logically consistent data stored and shared in an aspect of a given segment of reality [21]; they belong of various users, which contain information useful for indicated groups of system users,
T – technologies use in designing the information tool, which allow for further development of a system,
D – choice of technical and telecommunication devices, allowing to store information and guaranteeing its proper reception,
I – information characteristics and significance criteria, which should be fulfilled to guarantee proper information quality, including pertinence and redundancy,

U – usability, also defined as a functionality described as a measure of efficiency and effectiveness,
M – information management and set of systemic solutions used in a given social organization,
D – documentation describing the system,
R – relationships between particular data sets.

Each system should be evaluated, that is monitored and modified with regard to changing needs of its users. A waterfall model of software lifecycle speaks of five stages: requirements, design, implementation, verification and maintenance [22]. In reference to particular levels of software life cycle, before the information system supporting decision making starts being created, a design group should pay special attention to:

1. Thorough analysis of information needs reported by future system users; it is a key activity from the perspective of pertinence.
2. Tools evaluation criteria and usability.
3. Way of acquiring, gathering, processing and selecting information, which fulfill the significance criteria of features described by users (for example: timeliness).
4. Way of including future users in processes of design, learning, using and developing of a system.
5. Using innovative information technologies, in which a tool, that is information system, is designed, and adequate, from a user's perspective, selection of available devices, that will enable using the designed IT system.
6. Manner of organization and management of integrated information systems.
7. Technological aspects connected with, for example, system's operational efficiency or safety.
8. System maintenance costs, principles of profitability and costs related to the system using.

A major task of a group designing and IT system, being a tool for an information system, is guaranteeing system usability and quick interface service. The system is designed with a certain target group in mind; these are usually people in different age range and with different skills regarding the use of telecommunication devices [23]. In time of electronic economy, the availability of modern digital and electronic services, teleinformatic technologies caused that an increasing number of business processes is done with a use of electronic information exchange.

3. QUALITATIVE AND QUANTITATIVE EVALUATION OF THE INFORMATION SYSTEM

User's interface is a critical element enabling the evaluation of system usefulness for a potential user. Attributes used for a system evaluation by users are not always in line with a attributes recognized by experts [24] Qualitative evaluation is used for a set of elements:

$$QEISISS = \{Q, U , E, V, R\} \quad (2)$$

where:
QEISISS – qualitative evaluation of an information system having symptoms of integrated supporting system,
Q – qualitative evaluation of the software considering such features as: functionality, reliability, usability, efficiency, [25] maintainability, portability, [26]
U – evaluation of quality of usage by other features, such as: effectiveness, productivity, safety, satisfaction [27].
E – qualitative evaluation of available data bases with information; information quality measured based on features: significance, completeness, timeliness, access time, reliability, flexibility, comparability, processability, particularity, prioritization, confidentiality, relevance, pertinence, profitability [28, 29, 30]
V – value defined as the ratio between quality and price,
R - relationships between particular data sets.

Qualitative assessment is connected with costs, which include proper preparation of quality documentation, trainings, creating procedures and costs of warranties. A separated part of information systems is an IT tool, which is normally a complex computer software. A complexity of the software lies not in the programming language nor the tool's components, but it is a source of many problems related to quality and reliability. Most commonly, when referring to the programming issue, we analyze separately the intrinsic software quality and customer satisfaction. As much a s the satisfaction cannot be easily measured, it is different with the first category. A measure used for this purpose is often the number of bugs, time of infallible operation, or mean time to failure (MTTF)[31]. General quality model, described in the ISO 9126 norm, introduces the software quality model, which encompasses the entire production process life cycle, from the design to exploitation process. Three perspectives are distinguished here [32]:

1. Internal quality, which includes features that can be assessed based on the middle products, created in the production process,
2. External quality, which encompasses the features of software, perceived during the final product evaluation,
3. Quality in use, which includes features describing the level of fulfillment of user's business needs.

The quality norm defines a set of features, and each one of them corresponds with a certain category of functional and non-functional requirements set for the software. Measures based on these features can thus be based on a division: “has” or “does not have”. Efficiency measures allow to define the level of possessing certain features compared to an ideal situation. Controlling the level of fulfilling these requirements is presented in form of a report on various stages of a production process.

Systems are not evaluated only with regard to quality but also quantity, often referring to economic sciences. M. Szafrański defines economics as a “scientific sub-discipline dealing with economic issues connected with particular industry branches, types of economic activity or other systems defined in an economy on macro or micro level.” [33] J. Oleński presents the notion of information economics, as "particular economy defined according to a subjective-objective criterion. Its subjects are information, information processes and systems, and subjective scope encompasses all classes of social and economic entities, which participate in information processes and systems" [34]. Infonomics, in turn, refers to the area of [35]:

1. Cognition theory, that means learning and explaining the role of information in humans life,
2. Application, referring to practical use in information systems of rules of dealing with information with everyday life,
3. Education, defining the educating of a society to make more effective use of available information.

A research aspect of information economics is economy and attempts to analyze the economic justification of undertaken activities, also connected with economic profitability of information activity. Both information economics and infonomics enable the evaluation of undertaken activities and, as a result, the effective evaluation of the system.

Relating to the notions connecting IT issues with economy, we cannot overlook economic informatics, which was discussed in chapter 2 of this article. Further development of new technologies will most likely lead toward the development of new scientific domains, focusing not only on organizations and enterprises, but also, in wider understanding, on natural persons, their way of communication, as well as gathering and sharing information.

4. CONCLUSIONS

We must remember that quality is individually assessed by every user and levels of features values fulfilling the criterion of acceptability may vary for different groups of users. Quality is a subjective, content-related and varying category, [36] therefore it is hard to speak of one measure of evaluation of utility

and quality of a system for every user. Users from every segment should evaluated the system by assessing: quality of the software, quality of usage, quality of information included in the system or the value of the information system itself. First system evaluation should be made already at the system testing stage, that is before its validation. Proper system evaluation, which makes it possible to adjust the system to changing needs of users, cannot be done without systematic and periodical evaluation of the system by particular groups of users. Fitting the data to the information needs of users is the key to success. Adjusting data to information needs of the users is a key to success. Therefore we should pay close attention to successive levels of system's evolution, beginning at the designing process, through testing and finishing at implementation of a software product. Adjusting the needs of users to the system functionality is connected with a relative cost. Maintaining and evolving the software has been steadily increasing and reach more than 90 percent of the total cost [37].

We are certainly entitled to say that information system play and increasing role, not only by supporting the managerial decisions, but more and more often serving the entire society. The redundancy of information and impossibility to find current and reliable information that we need in everyday use, forces enterprises to build databases with information fulfilling the measures of information features required by users, and on the other hand to integrate information into information systems presenting value to a final user. In future it would be wise to consider focusing on development of research regarding social and economic information systems.

REFERENCES

[1] Kauf S. (2003) *Zintegrowane systemy informacyjne jako narzędzie wspomagające integrację marketingu i logistyki*, Borowiecki R., Kwieciński M. [ed.] *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona (wybrane problemy teorii i prkatyki)*, Kantor Wyd. Zakamycze, Zamykacze, Poland, 423.

[2] Papińska-Kacperek J. [ed.] (2008) *Społeczeństwo informacyjne* Wyd. Naukowe PWN, Warszawa, Poland, 18.

[3] Kostas Stefanidis, Georgia Koutrika, Evaggelia Pitoura, (2011) *A survey on representation, composition and application of preferences in database systems,* ACM Transactions on Database Systems (TODS), Vol. 36 Issue 3, Article No 19.

[4] Chuchro E., Daszewski W. (2006) *Informacja w sieci* Wydawnictwo SBP, Warszawa, Poland, 113.

[5] Gałczyński J. (2006) *Pertynencja jako wspólny cel użytkowników i pracowników informacji*, *Praktyka i teoria informacji naukowej i technicznej*, Tom IV, nr 3 (15) / 1996, Poland, 14.

[6] Kisielnicki J. (2008) *Systemy informatyczne zarządzania*, Wydawnictwo Placet, Warszawa, Poland, 49.

[7] Więcek-Janka E. (2011) *Games and Decisions*, Wydawnictwo Politechniki Poznańskiej, Poznań, op. cit. 24-25.

[8] Ibid.

[9] Radosiński E. (2001) *Systemy informatyczne w dynamicznej analizie decyzyjnej*, Wydawnictwo Naukowe PWN, Warszawa-Wrocław, Poland, 55.

[10] Wyrcza S. [ed.] (2010) *Informatyka ekonomiczna. Podręcznik akademicki.* PWE, Warszawa, Poland, 26.

[11] Ibid. 27.

[12] Szewczyk A. [ed.] (2007) *Społeczeństwo informacyjne – problemy rozwoju,* Diffin, Warszawa, Poland, 10.

[13] Kram E. (2007), *System informatyczny zarządzania. Projekt koncepcji systemu* Towarzystwo Naukowe Organizacji i Kierownictwa, Toruń, Poland, 24.

[14] Goliński M., Szafrański M., Graczyk M., Rosiński-Pusiak M., Miądowicz M. (2009) *Chosen system of access to information and their influence on formation of the quality of life in urban area* G. Dahlke, A. Górny [ed.] *Health protection and ergonomics for human live quality formation,* Publishing House of Poznan University of Technology, Poznan, Poland, 9.

[15] Ph. Kotler (2005) *Marketing*.,Rebis, Poznań, Poland, 575.

[16] Oleński J. (2003) *Ekonomika informacji. Metody*. Polskie Wydawnictwo Ekonomiczne, Warszawa, Poland, 43.

[17] Goliński M. Kałkowska J. (2003) *The usage of CRM system at modelling quality of products (CRM FQ - Customer Relatrionship Management for Quality)* : Human - Centred Computing: Cognitive, Social and Ergonomic Aspects: Proceedings of HCI International 2003 10th International Conference on Human-Computer Interaction Symposium on Human Interface, Japan, 2003 : 5th International Conference on Engineering Psychology and Cognitive Ergonomics : 2nd International Conference on Universal Access in Human - Computer Interaction, Crete,Greece,. - London LEA, op. cit. 986.

[18] Karwatka T. (2009) *Usability w e-biznesie*, Wydawnictwo Helion, Gliwice, Poland, op. cit. s. 9.

[19] Kisielnicki J., Sroka H., *Systemy informacyjne biznesu*. Agencja Wydawnicza Placet, Warszawa, Poland, 225.

[20] Ibid.

[21] Wyrcza S. [ed.] (2010) *Informatyka ekonomiczna. Podręcznik akademicki.* PWE, Warszawa, Poland, 255.

[22] Jaszkiewicz A. (1997), *Inżynieria oprogramowania*, Helion, Gliwice, Poland, 16.

[23] Under the notion of telecommunication devices we understand the devices which enable communication with a use of radio waves, that is those, which also allow for a

free use of Internet resources and online applications enabling acquiring information from systems, such as smart phones, palmtops, tablets, cell phones.

[24] Jagielski J. (2005) *Inżynieria wiedzy*, Uniwersytet Zielonogórski, Zielona Góra, Poland 203.

[25] Szafrański M. (2006) *Skuteczność działań w systemach zarządzania jakością przedsiębiorstw.* Wydawnictwo Politechniki Poznańskiej, Poznań, Poland, 17.

[26] ISO/IEC 9126:2001 *Software engineering – Product Quality, Part 1: Quality Model*, ISO, Geneva, 1998-2001.

[27] Ibid.

[28] Obora H. (2010) *Wybrane problemy pomiaru jakości informacji*: Borowiecki R., Czekaj J. [ed.] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, Warszawa, Poland, 122-127.

[29] Kolegowicz K. (2003) *Wartość informacji a koszty jej przechowywania i ochrony*: Borowiecki R., Kwieciński M. [ed.] *Informacja w zarządzaniu przedsiębiorstwem*, Kantor Wydawniczy Zakamycze, Zakamycze, Poland, 55.

[30] Kisielecki J., Soroka H. (2005) *Systemy informacyjne biznesu. Informatyka dla zarządzania* Placet, Warszawa, Poland, 35-39.

[31] Sosińska-Klata B., Chuchro E., Daszewski W. [ed.] (2006) *Informacja w sieci. Problemy, metody, technologie*. Wyd. SBP, Warszawa, Poland, 120-121.

[32] Sacha K. (2010) *Inżynieria oprogramowania* Wyd. Naukowe PWN, Warszawa, Poland, op. cit. 306.

[33] Szafrański M.(2007) *Elementy ekonomiki jakości w przedsiębiorstwach.* Wydawnictwo Politechniki Poznańskiej, Poznań, Poland, op.cit. 18.

[34] Oleński J. (2001) *Ekonomika informacji. Podstawy*, PWE, Warszawa, Poland.

[35] Czekaj J., Ćwiklicki M. (2009) *Infonomika jako dyscyplina naukowa*, E-mentor nr 2(29)/2009
http://www.e-mentor.edu.pl/artykul/index/numer/29/id/628
25.02.2011

[36] Papińska-Kacperek J. [ed.] (2008) *Społeczeństwo informacyjne.* Wyd. Naukowe PWN, Warszawa, Poland, 77.

[37] D. Plakosh and G. Lewis (2003) *Modewrnizing legacy systems: Software technologies, engineering process and business practices*. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA.

EXPECTED CHANGES IN THE FUNCTIONALITY OF IT SOLUTIONS IN THE AREA OF KNOWLEDGE MANAGEMENT IN SELECTED ENTERPRISES OF MECHANICAL ENGINEERING INDUSTRY

Adam Gumiński, Wojciech Zoleński

Institute of Management and Administration, Faculty of Organisation and Management, Silesian University of Technology

Abstract. The article presents the problem of the necessary changes in the functionality of IT solutions in enterprises of mechanical engineering industry. On the base of the survey questionnaire the analysis was undertaken to establish the determinants of IT applications functioning in selected enterprises of mechanical engineering industry. Desirable changes in the functionality of IT solutions supporting knowledge management were identified, including the analysis of the effectiveness of their implementation.

Keywords: Knowledge management, mechanical engineering enterprise, functionality of IT solutions

1. INTRODUCTION

IT tools used in the activity of manufacturing enterprises are an important component of management infrastructure. It is hard to imagine an efficient management in the current market situation without IT solutions in various spheres of business. It derives from the need of processing huge amounts of diverse information needed in business processes. Implemented solutions are mainly the support of operational activity and planning processes. Growing importance of knowledge management or simply, in some companies, aiming the objective to create a learning organization seems to be inevitable to increase the involvement of information technology [1, 3]. It is expected to intensify work on the functionalities of information systems that will strengthen knowledge management processes, which in turn will improve the functioning of enterprises. The important issue is the future vision of the company and managers' decisions in the area of development of functional systems corresponding to that vision. Likewise in many aspects of activity, the area of information infrastructure has limited resources and the question is to make the right choices based on effectiveness criteria.

In this article selected results of questionnaire survey on knowledge management processes in enterprises of mechanical engineering industry were discussed. The main purpose of the undertaken analysis was to determine the conditions and prospects of changes in the functionalities of information systems from the perspective of the enterprises.

2. KNOWLEDGE MANAGEMENT PROCESSES IN AN ENTERPRISE

Determining the functionality of information systems should be based on careful analysis of processes involved in knowledge management in an enterprise of mechanical engineering industry. The management processes model assumes that the knowledge life cycle in an organization consists of the following processes: organizational knowledge acquisition, knowledge accumulation (codification, storage), knowledge transfer (distribution) and knowledge use [2, 3].

Knowledge resources acquiring enables the following actions:

- acquisition of knowledge outside the organization (the acquisition of other companies or hiring key personnel) and rental of knowledge (acquisition of knowledge from hired consultants or researchers),
- adaptation of knowledge gained from the outside of the organization is the result of the impact of external environment: the emergence of competitive products, new technologies, social and organizational change; acquisition in this way new knowledge requires openness to change and the availability of sufficient internal resources; adaptation of significant knowledge recourses requires information systems; they can be used to develop processes models obtained as the best practice and to support experts in solving problems,
- knowledge creation within the organization; learning is the most effectively conducted in groups (as the research result of Xerox's Palo Alto Research Center), and therefore an important link in creating a knowledge organization is the formal and informal groups and social networks - communities of practitioners, communities of experiences exchange; apart groups (networks) referring directly contacts it is possible to create groups of virtual users to share their knowledge making use of Internet technologies,
- creating new knowledge as a result of its processing can be performed by people (knowledge workers), computer-aided (e.g. by analytical systems) or performed automatically (e.g. by knowledge discovery systems); in the processes of knowledge codification and combining may also be used e-learning systems and decision support systems.

Knowledge accumulation beyond the people’s minds is possible only in reference to explicit codified knowledge. In contemporary systems knowledge in

electronic form is dominating. Codification is the process of externalization of human knowledge and forming it appropriately to facilitate the access to users. The basic problem of codification is the inability or unprofitability of transforming complex tacit knowledge into explicit knowledge. The significant barrier is the reluctance of employees to share their unique knowledge.

Knowledge transfer involves the transmission (sending knowledge to potential recipient) and knowledge absorption (assimilation for later use). It is important to distinguish codified knowledge transfer achieved mainly by electronic channels of communication and uncodified knowledge transfer (formal and informal meetings of staff, knowledge markets, mentoring programs etc.). The basic problem of knowledge transfer is a combination of the knowledge availability and the protection of confidential knowledge, which can be difficult especially in the case of uncodified knowledge. Generally, the benefits of universal access to organizational knowledge outweigh the losses caused by the knowledge disclosure.

Knowledge use takes different forms. Knowledge can be a commodity (e.g. licenses, consulting services), but in most cases, knowledge is created and processed to produce a specific value within the organization. Many studies show that it is often the weakest link in the knowledge life cycle.

In European and American companies the knowledge processes model is the most often used, which clearly distinguishes and includes creation and processing of explicit knowledge and tacit knowledge [7], as well as the entire spectrum of knowledge combining of different degrees of openness and being codified. The reference to the disclosure of knowledge and capabilities of its codification can distinguish between two extremely different knowledge management strategies: codification strategy and personalization strategy. Selection of the correct proportions, and the separation of areas of both strategies is the basis for working out individual knowledge management strategy, taking into account the specificity of the company and its business goals. Codification is used in relatively stable business, in which the effectiveness (especially cost savings) can be achieved by repeatedly applying the best practices. Such an approach can lead to excessive routine, ossification and loss of knowledge not found in the formal procedures. Personalization is used in non-routine activities carried out under conditions of instability, in which efficiency can be achieved by innovation, rapid response to external impacts (opportunities and threats) and by taking into account the individual needs of the environment, especially customers. Codification strategy is better in the centralized structure of the company and usually involves large investments in centralized integrated IT systems. Personalization strategy is more adequate in the decentralized corporate structure. Information systems play a secondary role and can be largely decentralized, which is associated with limited expenditures on information technology.

Knowledge management is the principle of knowledge separation which is specific to problems that are solved in an enterprise from knowledge management tools that are relatively universal and to a large extent independent of the solved problems. This concept is applicable to systems based on knowledge (knowledge based system, KBS) [4, 5].

For knowledge (as opposed to simple data) high level of understanding and high level of generality of the implementation context is characteristic. Between classification and typological characteristics and explaining cause and effect relationships the feedbacks are: to organize and generalize the facts that helps formulate the laws (nomological dependences) or at least research hypotheses for the discovery of new laws; knowledge of rights (e.g. cause and effect relationships) in a natural way arranges the facts and helps to carry out their classification and typology.

3. THE SCOPE OF FUNCTIONALITIES IN IT SOLUTIONS SUPPORTING KNOWLEDGE MANAGEMENT USED IN ACTIVITY OF ENTERPRISES OF MECHANICAL ENGINEERING INDUSTRY

The survey of knowledge management has been carried out during June-July 2011 in 12 selected mechanical engineering industry enterprises located in the Silesia province. The questionnaire survey was carried out in the form of direct interviews with top managers of selected enterprises. The main objective of questionnaire studies was to identify methods and tools used in knowledge management in selected companies, including the audit of applied IT solutions in key functional areas.

The studies brought the information which functionalities in the field of knowledge management are implemented in the IT solutions in analyzed enterprises and to get the knowledge what changes respondents (representing executives of these companies) suggest.

The majority of survey questions were concentrated on obtaining information about processes and tools for knowledge management in the following key areas of the enterprise's activity:

- human recources,
- production,
- research and development,
- logistics,
- market/customers,
- finance.

The fixed division derived from the applied IT solutions in the analyzed companies. Questions have been divided into several categories corresponding to the structure of knowledge processes in the surveyed enterprises [6]:

- business level (integration level),
- structural level,
- level of knowledge processes and tools (knowledge acquisition and development, knowledge codification, knowledge transfer, knowledge utilization,
- the audit of applied IT solutions.

Respondents who were senior executives pointed the highly differentiated advancement of knowledge management in their enterprises. In some enterprises full cyclical knowledge audits were made in recent years. In other enterprises respondents pointed the need of carrying out knowledge audits without a specific deadline for their realization. In most of analyzed companies you can observe the importance of implemented ISO 9001 and ISO 14001 management systems, which operate on the basis of information system processes. The personnel of analyzed companies use IT tools (Internet, Intranet) for developing knowledge management processes. But the road to overcome in this area is still long. The awareness of decision makers is particularly important. In many cases the interviewed managers emphasized the importance of information and knowledge as key factors for the development of the company, but implementation knowledge management is regarded by them as a problem that can be put aside for the future. Managers rightly believe that knowledge management infrastructure requires large amounts of time and money, and the positive effects often have to wait long.

In mechanical engineering industry enterprises, the lathe and assembly production of high complexity is often carried out. The unitary production has a large share, including the production of large machines, primarily as to make to order. In addition, the activity of these enterprises is particularly sensitive to changes of economic conditions. These circumstances have a significant impact on the functionalities of systems applied in these enterprises. In the first stage most companies implemented financial-accounting and personnel systems. In the next stage they implemented sales, purchasing and materials management systems, which functionalities are largely independent of the nature of the business. In all surveyed enterprises CAD systems are exploited.

It should be noted that the most important information systems related to the core business of an enterprise are implemented as the last and bring a lot of problems. Relatively frequent you can observe the situation when the module related to production management in manufacturing companies (not only in mechanical engineering industry enterprises) is not implemented despite exploiting MRP/ERP systems.

The overview of the functionalities of applied solutions indicates the evolutionary implementation of specific modules in selected areas of the studied enterprises. Implemented functionalities are mainly focused on operational activities.

4. THE REASEARCH OF CHANGES PROSPECTIVES IN KEY FUNCTIONALITIES IN ACTIVITY OF ANALYSED MECHANICAL ENGINEERING INDUSTRY ENTERPISES

It seems to be inevitable for a modern manufacturing enterprise to strive for company's formula based on knowledge. The growing awareness of this fact among executives is very important. Therefore, any changes in the scope of functionalities of IT solutions supporting knowledge management should be carefully analyzed and adapted to the business development strategy, taking into account the knowledge management criteria. It is necessary to answer the question of what knowledge processes should be strengthened, to what extent and in what timescale.

An interesting question is how to understand the concept of "functionality development". This concept can be interpreted as the introduction of evolutionary adjustments in already implemented IT solutions. You can also try to optimize the solutions according to the criterion based on a particular purpose. Sometimes small changes can significantly improve the effectiveness of previously implemented solutions. However, the most often understood development of the functionality is the implementation of completely new, radical changes in applied IT solutions.

Each of these scenarios requires a different approach, but in each case the key objective should be strengthening the knowledge processes, particularly those that significantly improve business processes. Any change to the functionality is associated with specific contexts and success determinants of implementation in a specific enterprise. Each time a change of functionality requires to provide not only the layer of information technology, but also prepare personnel to operate the modified functionality [5]. A serious mistake is to make changes to the functionalities without the simultaneous preparation of the future users. Only the appropriate coordination of these two elements can bring expected benefits.

The key issue in the implementation process is to determine the criteria by which a decision is made. These criteria are closely linked with the expectations of policymakers. The criterion of economic effectiveness is most often used. The most desirable are the benefits that bring in the short term economic effects in the form of cost reductions or employees' time waste reduction. However, the synergistic effects resulting from the implementation of modern solutions are obtained in the long term. These effects can include: improvement of productivity, information processing efficiency and work effects.

Working out and implementation of changes in the functionalities in a particular enterprises is a unique task and therefore requires a methodical approach. A good practice would be to identify the characteristics of modified functionality, which would include the following elements:

- main objectives of functionality implementation,
- sub-goals of functionality implementation,

- circumstances of functionality implementation
- target users of the functionality,
- input information
- processing algorithms,
- output information,
- effects of the functionality implementation.

In mechanical engineering industry enterprises in the process of determining functionalities changes the procedure may be applied, shown schematically in Figure 1. Scheme comprises the following stages:

- the analysis of determinants of functionalities changes,
- the analysis of business processes,
- the analysis of decision making processes,
- the analysis of knowledge management processes,
- determination of possible changes in the functionalities of the system supporting knowledge management,
- the analysis of effectiveness of selected functionalities implementation in system supporting knowledge management,
- decisions on accepting or rejecting changes of the selected functionalities of the system supporting knowledge management.

The stage „The analysis of determinants of functionalities changes" includes the audit of organizational and technical infrastructure and the assessment of the information preparation of potential users of modified functionality of the system supporting knowledge management.

The stage „The analysis of business processes" includes the audit of business processes realized in an enterprise in order to determine knowledge deficit in analysed processes.

The stage „The analysis of decision making processes" includes the audit of decision making processes realized in an enterprise in order to determine knowledge deficit in analysed processes.

The stage „The analysis of knowledge management processes" includes the audit of knowledge management processes realized in an enterprise in order to determine knowledge deficit in analysed processes.

The stages focused on the analysis of business, decision making and knowledge management processes and the diagnosis of the current and the target state taking into account managerial decisions for medium-and long-term prospects for the company should be performed. Audits conducted in the above mentioned processes areas allow to determine what knowledge processes need to be strengthen and what modifications are necessary. On each of the outlined stages it should be searched the opportunities of analysing and changing the functionalities of a computer system to improve knowledge management in the enterprise.

The stage „Determination of possible changes in the functionalities of the system supporting knowledge management" includes the initial determination of possible changes in the functionalities of the system supporting knowledge management with the identification of specific actions to be taken for their implementation.

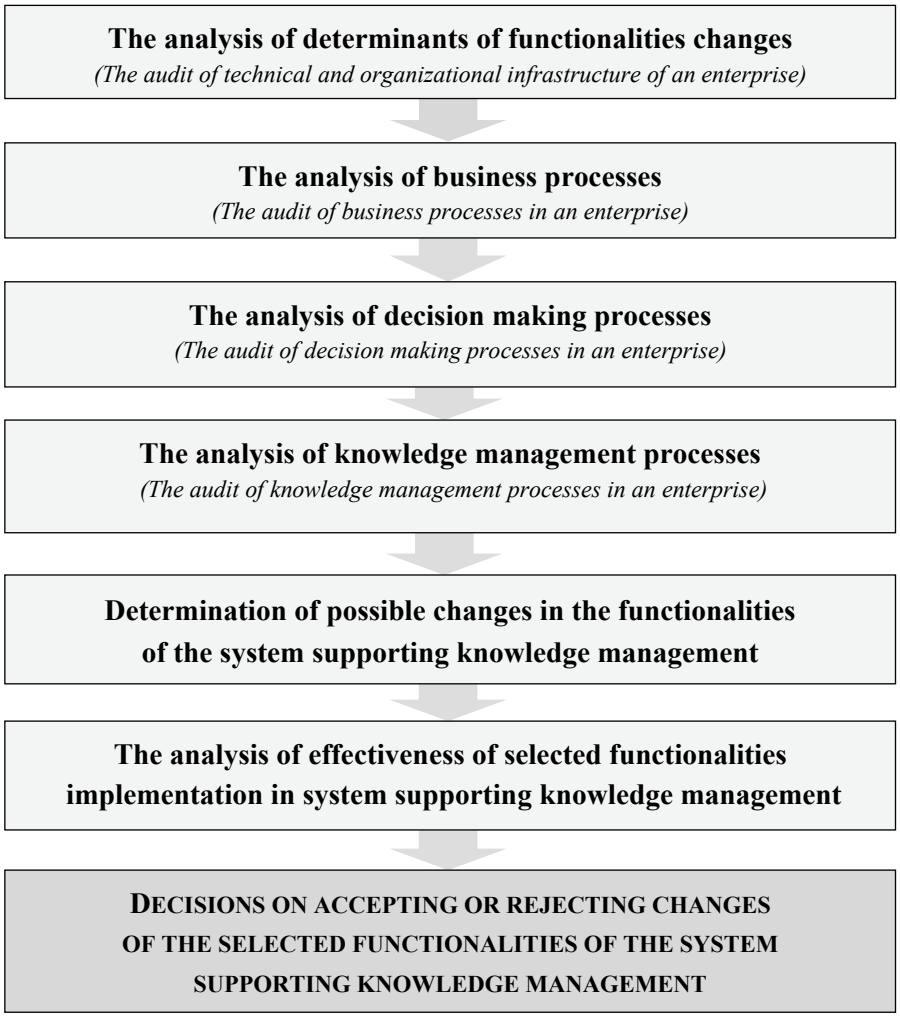

Figure 1. The scheme of procedure for determining changes in the functionalities of the system supporting knowledge management in an enterprise of mechanical engineering industry.

The stage „The analysis of effectiveness of selected functionalities implementation in system supporting knowledge management” includes the analysis of selected functionalities in terms of technical and economic effects.

The stage „Decisions on accepting or rejecting changes of the selected functionalities of the system supporting knowledge management” closes the process of determining changes in the functionalities and represents a milestone for the further development of the concept of functionalities changes and its subsequent implementation.

Based on the survey it can be concluded that the surveyed respondents decide for the solutions effective in the short term, despite the full awareness that knowledge management is more effective in the long term. The choice of the short-term prospect of the implemented functionality results from expectations about economic effects.

Suggested changes in the functionalities of IT solutions focused on improvement of business processes on the operational level. Proposals for changes were significantly different because of the technological level of the company, which primarily resulted from the implemented applications. In the majority of cases respondents agreed in their expectations about the necessity to search evolutionary changes in functionalities. None of the respondents pointed out the need of implementing a fully integrated system at present development stage of a company.

The expected development of information systems in enterprises of mechanical engineering industry can be divided into two areas. The first ("hard") is related to the computerization of the core business, particularly the improvement of production management systems. The second area ("soft"), in which new functionalities of information systems are expected to support relationships with contractors. In the unitary production the business profitability is affected by a great deal of different factors of low stability, particularly the order book, the parameters of the contracts concluded with customers (unitary price of a product can be very different), the parameters of contracts with suppliers and subcontractors (prices can also be very different). For the conclusion of beneficial contracts and not for unfavorable ones, you should have extensive knowledge about production costs and production capacity. inventory levels and supply capabilities and knowledge of potential suppliers and cooperators (as broad as possible the list of subcontractors and suppliers, information about their reliability, costs, a willingness to cooperate, the potential negotiation).

5. CONCLUSION

Changes in the functionalities of applied IT solutions for knowledge management in enterprises of mechanical engineering industry are inevitable and form a continuous process resulting from the adaptation of business processes in an enterprise to dynamically changing external and internal conditions. The analysis of the responses of the majority of respondents indicates the expectations of the functionalities of the system not fully integrated, but properly prepared to meet the needs of a specific company. The efficiency criterion in the field of knowledge management indicates too high financial and non-financial inputs in relation to achievable effects for integrated systems.

To ensure high efficiency of the implemented changes in the functionalities of IT solutions it is necessary to undertake a deep analysis, which should answer the following questions:

- What functionalities are necessary to implement in the context of strengthening the knowledge processes in a specific enterprise?
- What are the criteria of choosing the functionality?
- What is the level of preparation of the technical infrastructure and human resources to implement new functionalities?
- What actions should be undertaken for effective implementation and in the longer term to optimize making use of the implemented solutions?

Based on the studies in selected enterprises of mechanical engineering industry it can be stated that any functionality reconstruction of information systems requires a methodical approach. In order to determine the functionality development you could use the procedure proposed in the fourth section of this article.

Long-term effectiveness of implemented changes in functionalities supporting knowledge management in enterprises of mechanical engineering industry are largely dependent on the applied technology and adequate preparation of personnel benefiting from these solutions. Unfortunately, in most of the analyzed companies it was observed the tendency of managers to make decisions about the functionalities changes based on criteria focused on short-term effects, generally on economic criteria. Implementation of the functionalities changes of information systems should be treated as the investment in the area of knowledge processes, which could bring synergy effects resulting from more efficient use of corporate resources.

The publication is financed from public science funds in the years 2010-2013 as the research project No. 03-0112-10 /2010 dated 09.12.2010.

REFERENCES

[1] Evans Ch. (2003) *Managing knowledge. HR's strategic role*. Butterworph – Heinemann.

[2] Gołuchowski J. (2007) *Information Technologies in knowledge management in organizations.* Wydawnictwo Akademii Ekonomicznej. Katowice.

[3] Jashapara A. (2006) *Knowledge management.* PWE. Warszawa.

[4] Jemielniak D., Koźmiński A. (2008) *Knowledge management.* Wydawnictwa Akademickie i Profesjonalne. Warszawa.

[5] Kisielnicki J. (2008) *Management Information Systems*. Wydawnictwo Placet. Warszawa.

[6] Kowalczyk A., Nogalski B. (2007) *Knowledge management. Conception and tools.* Diffin. Warszawa

[7] Nonaka I., Takeuchi H. (2000) *The Knowledge-Creating Company. How Japanese Companies Create the Dynamics of Innovation*. POLTEXT, Warszawa.

EVALUATION METHODS OF IT INVESTMENT IN ORGANIZATION

Tomasz Ordysiński

Institute of IT in Management, University of Szczecin

Abstract. The main issue of this article is presentation of different evaluation methods of IT investment in enterprise. In the first group are presented methods based on indexes such as EIF, EIC, NPV, IRR ROI and Real Options calculation. The second class of methods deals with IT cost management and is based on TCO (Total Cost of Ownership) methodology. The next of presented methods, BSC IT (IT Balanced Scorecard), enables managers to locate IT in the enterprise development strategy and to estimate "Value Added" of IT solutions. The last type is based on Business Process Reengineering enabling managers to completely understand direct and indirect advantages of planned investment.

Keywords: evaluation of IT investment, IT Balanced Scorecard, Business Process Reengineering

1. INTRODUCTION

Since a long time, as presented by Gartner Group reports, there is a communication problem and a lot of misunderstandings in the issue of IT role in enterprise. The difficulties in presentation of capabilities of computer applications and it's value for business often causes a situation, when IT strategy is based on just keeping existing infrastructure running. Among managers there is a very common vision of IT as an extremely expensive project – the perspective of reasonable investment in building market value of organization is not noticed. Proper attitude towards IT resources management should be started from identification of its advantages. First of all computer systems allow to optimize existing business model by supporting business processes (e.g. area of Customer Relationship Management, Research and Development or Supply Chain Management). Implementation of proper IT solutions increases productivity, decreases operational costs, improves quality and customer satisfaction. All those advantages give direct rise to the increase of market share and improvement of the competitive position. There is a common belief that IT investment is a good idea but there are problems in identification of direct advantages of such an expenses (results can be visible after some period). Very often clear "accountancy" calculation stops interesting, long time IT investment – cost are visible at once.

The goal of this article is the review and short presentation of evaluation methods of IT investments focused both on cost and benefit side. There are presented calculation based on indexes (EIF, EIC, FV, NPV, IRR, ROI), Real Options Method, TCO (Total Cost of Ownership), BSC (Balanced Scorecard) and BPR (Business Process Reengineering).

2. BENEFITS CALCULATION OF IT INVESTEMENT – APPLIED INDEXES

Financial analysis of any IT project should be started from studies of organization performance without any proposed changes (base case). Then the company can check all available options identifying possible cash flows. The value of IT project in that case is a simple difference in amount of money. From the technical point of view this is a difference of the net discounted cash flows, corrected with the risk between situation without any IT changes and possible situations of the company created by any proposed option. The evaluation of IT project means from one point of view, that one must measure its efficiency, and from the second point index analysis based on dependable financial measures. Between terms efficiency and productivity is a significance difference. Efficiency concerns the issue of performed task/process and productivity describes the way the process is performed. For example introduction of new IT system gives opportunity of preparation more detailed report (efficiency increase) in shorter time (productivity increase). Both effects can be considered in quantity and quality categories. Quantity results are defined in certain units (e.g. money). The quality results are much more difficult to measure – the financial value can be only assumed.

The basic questions, which must be answered in case of IT investment is how much it adds to the value created by organization, when and whether it will create any profit. Only processes supported by the future solution in organization should be evaluated – in other areas in the company there usually is no economic justification for specified expenses. Introduction of new IT solution can have two basic goals. The first one is cost reduction e.g. the company can reduce cost of warehouse. The second is to increase the added value e.g. by quality improvement which can cause bigger market share [1].

The profitability of investment is measured by comparison of expenses to gain profit. If both can be given in the same units, then we can calculate Financial Effciency Index EI_F, which is relation of investment positive effects (E) to the expenditures (N):

$$EI_F = \frac{E}{N} \tag{1}$$

When the number is bigger than 1 that we can say that our investment is financially efficient [2].

Some advantages of IT implementation are so hard to measure that are treated as immeasurable effects. When the goal of the investment is not financially defined then the efficiency in money is not possible to calculate. In that case we can assume that if our (not financially defined) goal is achieved and the planned budget is not exceeded then the efficiency of our project is acceptable. This is described with the index of goal effectiveness coefficient EIC proposed by A. Wargin. This index does not have to be a number and can describe the level of investment efficiency. The calculation process is proceeded in steps:

1. After the project is finished there must be identified the goal realization ratio and checked, whether the total expenditures are not higher than planned;
2. Realization of goals in 100% and meeting the budget limitations means that the project was efficient;
3. In case of not reaching all planned goals one can identify the realization ratio. After assigning wages to all planned goals the total efficiency ratio can be calculated.[3]

IT investment, as all kind of new project in organization, has some risk. The level of the risk depends on competitive possibilities of money investment, which can give smaller profit but are 100% dependable. An example of such a alternative are debentures or bank deposits. Those alternatives give company the value of discount rate, which is used in analysis of IT investment – we can answer a question what is the present value (*PV*) of money which we can gain after some period (*FV*). The calculation formula:

$$PV = FV * a_t, \tag{2}$$

$$a_t = \frac{1}{1 + r*}, \tag{3}$$

where:

a_t – discount factor, r – discout rate, n – number of periods [4].

The current worth of a future sum of money or stream of cash flows given a specified rate of return is used for calculation of Net Present Value (NPV). NPV compares the value of a money today to the value of that same money in the future, taking inflation and returns into account. If the NPV of a prospective project is positive, it should be accepted. However, if NPV is negative, the project should probably be rejected because cash flows will also be negative. The formula:

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+r)^2} \tag{4}$$

where:

B_t – incomes in year t, C_t – costs in year t (including investment expenditures, without depreciation), n – number of periods [5].

The second commonly used indicator is *IRR* – Internal Rate of Return as the rate of growth a project is expected to generate. It can be helpful in situation, when *NPV* of the set of considered IT project is equal zero. Generally speaking, the higher a project's internal rate of return, the more desirable it is to undertake the project.

The formula:

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+IRR)^2} = 0 \tag{5}$$

where:

B_t – incomes in year *t*,

C_t – costs in year t (including investment expenditures, without depreciation),

IRR – Internal Rate of Return [6].

For the investors, who support extremely expensive IT projects, the return on the investment is a crucial issue. One of the most popular indicators is ROI (Return on Investment). However there is a lack of universal method of ROI calculation for IT projects. Some "model " attitude can be described as:

$$\text{ROI} = \Delta\text{Income} - \Delta\text{Cost} + \text{immeasureable benefits} - \text{IT expenditures} \tag{6}$$

where:

ΔIncome – changes in income before and after IT project caused by IT implementation,

ΔCost – changes in cost level before and after IT project project caused by IT implementation,

immeasureable benefits – quality parameters usually with subjective evaluation (e.g. benefits caused by higher employee satisfaction),

IT expenditures – all costs of IT investment and maintenance [7].

Usually the IT project has some different variants to be chosen and applied. Additionally there is always option when organization decides to invest the money into e.g. bank deposit or stock market. The problem is how to measure which investment will give higher profit. The solution can be Real Option method.

3. VALUATION OF IT PROJECTS USING REAL OPTIONS METHOD

Evaluation of an IT project requires application of proper methods of efficiency assessing, whereas the traditional methods based on discounted cash flows do not take into account the specificities of contemporary IT projects. Specificity that distinguishes IT projects from other capital investments consist of: high uncertainty of benefits, investment cost irreversibility and flexibility of the implementation process (understood as the possibility of modification of this process). The

specificity of IT projects arises due to the peculiarity of information system as a product of the project, the characteristics of the methodologies of implementation projects, the character of effects provided by the computer system and the nature of the technology applied [8].

Among the ways and directions of improvement of the evaluation process of IT investment, there is one that focuses on the applicability of methods developed and used in other areas of science. One of the proposals presented in the literature is to assess the effectiveness of IT projects using real options method [9].

The concept derived from financial markets, based on the conception of financial options. An option is a contract between a buyer and a seller that gives the buyer the right—but not the obligation—to buy or sell a particular asset (the underlying asset, e.g. stocks) at a later day at an agreed price. In return for granting the option, the seller collects a payment (the premium) from the buyer. A call option gives the buyer the right to buy the underlying asset; put option gives the buyer of the option the right to sell the underlying asset. If the buyer chooses to exercise this right, the seller is obliged to sell or buy the asset at the agreed price. The buyer may choose not to exercise the right and let it expire. The underlying asset can be a piece of property or shares of stock or some other security.

There is a set of properties characterizing capital investments, which predispose those investments to be evaluated using a real options method. Those properties are:

- high uncertainty of the benefits of investment,
- investor decision-making flexibility,
- irreversibility of investment cost,
- obtaining through the project additional effects or further investment opportunities (indirect effects).

Due to their properties, here come the systems which are particularly marked out for evaluation using options method:

- Due to the particularly high uncertainty of outcomes: strategic systems (referred to in subsequent classification schemes respectively as: strategic information systems, systems providing innovation benefits, strategic systems, strategic applications, applications with high potential).
- Due to the project by obtaining additional investment opportunities - infrastructure systems.
- Due to the irreversibility of the costs and flexibility of investor decision-making any type of system can be distinguished [10].

Summarizing the issues, the real options method is particularly useful for assessing infrastructure systems and systems of strategic nature. These conclusions coincide with the cases reported in the literature.

All above presented methods focused on the benefit side of IT investment – the side of cost was limited to simple approach of summarizing amounts (expendi-

tures) caused by IT department in organization. However, the research of Gartner Group (GG) consultant showed that only 10-15% of money spent on IT project is in decision power of IT managers [11]. The rest is cost of bigger, interdepartmental initiatives, in which computer application or hardware is a part of expenditures. For that reason complex attitude was required and GG proposed a TCO (Total Cost of Ownership) method.

4. IT COST IN ORGANIZATION – TCO METHOD

According to new, reasonable trends of concerning IT in organization, the role of computer hardware and software is to support existing business processes. And this is a place where advantages of IT can be noticed. The same situation can be considered in a matter of IT costs. GG researched showed that most of those cost are generated outside IT departments, mainly by end-users e.g. awaiting time for network delays, system suspend etc. The level of those indirect expenditures can reach the amount directly connected with IT initiatives.

The revelation of indirect cost requires global attitude towards IT role in organization and IT cost management. The solution can be TCO method, which enables managers to take complex look at the matter of implementation, development and maintenance of IT resources in enterprise. TCO proposed by Gartner consists of:

- System of cost classification, containing a list of direct and indirect costs;
- Statistical data bases containing information about IT cost from many branches. It is used for benchmarking (comparing to the best in particular branch);
- Methods of cost analyzing and planning;
- Set of “best practices” in a form of recommendations for rational IT expenditures.
- Set of computer applications, which can automate the process of control and planning of IT project in the area of cost [12].

The most important part is the model of IT cost of ownership, cause it reveals a huge list of very detailed direct expenses in classes like: hardware and software, management, support, development and telecommunication. The indirect classes of cost are: end-user (self-learning, help of colleagues, self-programming etc.), suspension (planned or unplanned lack of service, system breakdown etc.). There is also implemented a kind of “user inactivity” – actions of system usage for private reasons.

The methodology of TCO consists of four steps closed in a loop:

1. Where is the organization today? (present state of IT expenses based in class model)
2. What is the situation in organization comparing to average in branch? (based on statistical data)

3. What can be done? (TCO model contains verified recommendations like resource stocktaking, helpdesk organization, SLA agreements, trainings for end-user and IT employees).
4. How efficient are changes applied? (control step checking changes in cost's profile) [13].

The method has been applied in Gartner software, which can assist in all presented steps and gives possibility of "what-if" analysis. It supports managers in planning and choosing IT solutions not only from the perspective of the functional and short term advantages but shows the IT costs in whole system life cycle.

As presented above the cost evaluation can be complex – including much more than typical accountancy calculation. However, to convince the managers of high expensive IT investment the advantages side should be properly presented. There is a set of methods to show IT positive influence on organization. One of them is Balanced Scorecard (BSC).

5. THE IT VALUE IN ENTERPRISE – BSC METHOD

The Balanced Scorecard is a method of efficiency measurement in organization performed in many perspectives. It is able to translate mission and strategies of the organization into measureable goals. The attitude was applied as Balanced It Scorecard, which presents the role of IT solutions in organization and it's influence on business. Small modifications put the IT initiatives into four perspectives of BSC: financial, customer, process and development. For example the mission of IT department is building the company value and improvement of customer's satisfaction. The customer, in case of IT dept., are business processes. Mission can be described as added value, innovation level or an income from specific customer. The management tools can be e.g.: identifying and building application portfolio, TCO or supply management.

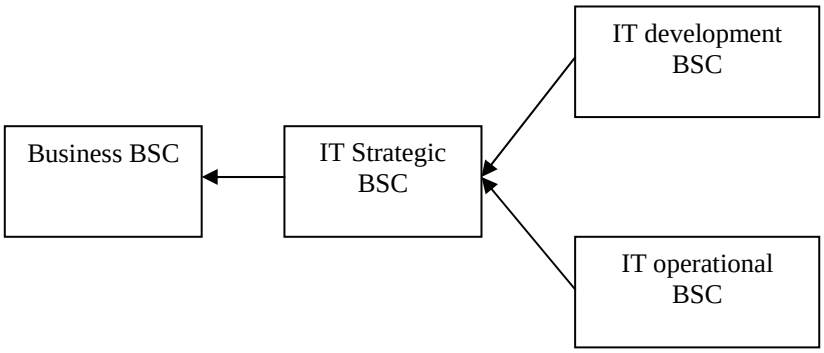

Figure 1. Cascade BSC. Source: Van Grembergen W.: The Balanced Scorecard and IT Governance. Information Systems Control Journal, 2000

Different types of BSC can be joint in cascade model to show complex transformation of strategy into IT operational goals. It very strong connects business and IT initiatives (Fig. 1)

Table 1. IT Balanced Scorecard

STANDARD IT BALANCED SCORECARD	
1. USER ORIENTATION How do users view IT department?	3. BUSINESS CONTRIBUTION How does management view the IT department?
MISSION To be preferred supplier of information systems	MISSION To obtain reasonable business contribution of IT investment
STRATEGIES Preferred supplier of applications Preferred supplier of operations Vs. proposer of best solution, from whatever source Partnership with users User satisfaction	STRATEGIES Control of IT expenses Business value of IT projects Provide new business capabilities
2. OPERATIONAL EXCELLENCE How effective and efficient are IT processes?	4. FUTURE ORIENTATION How well is IT positioned to meet future needs?
MISSION To delliver effective and efficient IT applications and services	MISSION To develop opportunities to answer future challenges
STRATEGIES Efficient and effective developments Efficient and effective operations	STRATEGIES Training and education of IT staff Expertise of IT staff Research into emerging technologies Age of application port folio

Source: Van Grembergen W.: The Balanced Scorecard and IT Governance. Information Systems Control Journal, 2000

As the perspectives of IT Balanced Scorecard can be defined:

- User orientation – end-user evaluation of IT system,
- Operational perfection – represents IT processes giving services,
- Financial investment of company – value of IT investment,
- Future orientation – human and technological resources which are necessary for proper IT service (Table 1).

Every of these perspectives can be expressed in specified measures and calculated to evaluate present situation. Those calculation should be performed in repetitively and compared with established goals. During the BSC construction there are established cause-reason connections between two types of measures: result and

directive. For example the result measure as the number of mistakes made by end-user should be connected with directive measure in form of number of trainee hours per user. Lack of such a connections would disable evaluation of efficiency of performed strategy.

The method of cascade connection of Balanced Scorecards is can be very suitable evaluation and management system for IT projects and it's direct connection (proof of necessity) with general business strategy and goals. However there is no direct information how IT will improve organization functioning – the proper method seems to be Business Process Reengineering (BPR).

6. BPR AS A IT PROJECT JUSTIFICATION

The term ''business process reengineering'' first appeared in the information technology (IT) field and has evolved into a broader change process. The aim of this radical improvement approach is quick and substantial gains in organizational performance by redesigning the core business process. In the 1990s, many US companies embraced reengineering as an effective tool to implement changes to make the organization more efficient and competitive. The motivation was usually the realization that there was a need to speed up the process, reduce needed resources, improve productivity and efficiency, and improve competitiveness.

Typical steps of Business Reengineering Process are:

1. determine Customer Requirements &Goals for the Process;
2. map and Measure the Existing Process;
3. analyze and Modify Existing Process;
4. design a Reengineered Process (identify IT levers);
5. implement the Reengineered Process [14].

The most common connection between BPR and information technology, which is presented in literature, is concerning IT as a support tool for process reengineering. There are many applications which give possibility of process modeling, analysis and optimization (e.g. ARIS, ARENA, ADONIS, IGRAFX or IBM tools). The Author's attitude is focused on the area of using BPR as a justification of new IT project – computer applications applied in new, more efficient process can double or even triple the final result. As the TCO points, that IT costs must be considered in whole organization then BPR advantages (supported by proper IT solution) can be an excellent tool to present holistic result of new IT investment.

Business process modeling can be joint with Balanced Scorecard – both of them require clear and understandable measures. In case of BPR three usually dimensions of the process are optimized: time, costs and quality. The positive effect of IT implementation can be presented in two kinds of future process options: with or without IT support. The deference between directive measures (defined goals) will clearly show positive result planned IT project.

$$\text{IT investment results} = \begin{array}{c}\text{benefits of reengineered IT supported processes}\end{array} - \begin{array}{c}\text{benefits of reengineered processes without IT support}\end{array} \quad (7)$$

7. CONCLUSION

The rapid evolution of information technologies and its declining costs are creating opportunities to change and improve the way enterprises conduct business. Usually such a change requires development or purchase of new IT resources. The goal of this article was to present a set of different methods used for evaluation of IT investment. First group based indexes gives a manager possibility to measure IT project but only from the financial point of view. In that group there is no method which would help to reflect indirect advantages of such a investment. However an interesting attitude is using real options methods to compare different alternatives of decision. The following classes of presented methods, like TCO, BSC or BPR, focus on complex analysis of organization in dimension of costs and efficiency.

Finally the question must be asked, which method is the best and should be commonly used. There is no simple answer – each IT investment has unique features which determine usefulness of some presented methods because of available data, risk level or just cost of applying specific method. However, the truth is that the more decision-maker knows about future results of his investment the less surprised he will be. In Author's opinion methods, which create complex view (include indirect costs and advantages) should be applied in a first place – especially in case of IT initiatives which influence whole organization. Class of index based evaluation methods should be treated as kind of helpful but not crucial information.

REFERENCES

[1] Powell P. (2008) *Information Technology Evaluation: Is It Different?* The Journal of the Operational Research Society, Palgrave Macmillan Journals, UK.

[2] Financial Efficiency Index, `http://www.investopedia.com/`

[3] Wargin A. (2003): *Exercise of calculating ... profitability*. Pckurier 8/2003 (in Polish).

[4] Present Value. . `http://www.investopedia.com/`

[5] Net Present Value. . `http://www.investopedia.com/`

[6] Internal Rate of Return. . `http://www.investopedia.com/`

[7] Return on Investment. . `http://www.investopedia.com/`

[8] Łukaszewski T. (2008), Real *Option methods in planning of IT investment*. Doctor thesis, University of Szczecin, Poland 2008 (in Polish).

[9] Łukaszewki T. (2003) *Characteristic of IT project versus it's evaluation with Real Option Methods*. SWO Katowice, POLAND (in Polish).

[10] Lee J., Paxson D (2001)., *Valuation of R&D* Real American Sequential Exchange Options, R&D Management, vol. 31 no. 2, US.

[11] Gartner Group (2009) `http://www.gartner.com/`

[12] Dabbs T. (2008) Optimizing Total Cost of Ownership (TCO). `http://www.chemshow.com/`

[13] Comparing and Selecting Solutions Using TCO Analysis. (2010) `http://www.alinean.com/`

[14] Attaran M. (2004) Exploring the relationship between information technology and business process reengineering. Information & Management 41, Elsevier, Holland.

APPLICATION IMPLEMENTING THE UCON MODEL FOR SECURITY OF INFORMATION SYSTEMS

Aneta Poniszewska-Marańda

Institute of Information Technology, Technical University of Łódź

Abstract. The aim of this paper is to analyze and illustrate the problem of implementation of UCON model for the security of information systems. The UCON model is a fairly new concept introduced to provide a comprehensive approach to the issue of access control. The model as such is purely abstract, which potentially leads to a diversity of implementation methods.

Keywords: Security of Information Systems, Access Control, Access Control Models, Usage Control, UCON model

1. INTRODUCTION

Information system is a method and infrastructure of communicating information. Its main objective is to share, collect, process, store and display information. Their main application in business organizations is to carry out organization's missions, achieve goals and measure as well as control performance. With pervasiveness of technologies grows a higher demand for appropriate security of data stored and used in information systems.

Since the value of information is constantly growing more and more businesses are in need for information system to aid them with information gathering and processing. The most important issue that arises here is how to ensure safety of this data that may be held on servers, personal computers or PDAs (Personal Digital Assistant). This is where access control comes in. The main role of access control is to ensure that no unauthorized user will be able to gain access to resources and be able to copy or modify them. It ensures proper protection for information held within the information system so that no individuals or companies will be able to steal or use it. There are currently many models of access control that suggest rules of guarding data from unwanted guests that we may choose from and still more are developed. Every company should analyze their needs and choose best suitable model for their needs to ensure safety and confidentiality of sensitive data.

The aim of this paper is to analyze and illustrate the problem of implementation of UCON (Usage Control) model for the security of information systems.

The proposed solution to the given task includes the development of exemplary application.

The paper is divided as follows. The first part presents an overview of the problem of access control, and is followed by a short description of the UCON model. This model is a fairly new concept introduced to provide a comprehensive approach to the issue of access control. The model as such is purely abstract, which potentially leads to a diversity of implementation methods. Next, the idea of solving the problem is presented. The demonstrative exemplary application was created – a web application that is an online music store, with the main focus at the problem of file usage control policies grounded on UCON. Finally, the technical details of our solution are analyzed.

2. ACCESS CONTROL FOR INFORMATION SYSTEMS

Higher demand for appropriate security of data stored in different information systems grows with pervasiveness of information and business technologies. Information system is a method and infrastructure of communicating information. Its main objective is to share, collect, process, store and display the information. Their main application is in business processes – information systems help carry out organization's missions, achieve goals and measure as well as control performance.

There are many types of information systems, and one organization may use more than one to satisfy their needs. The main kinds of those systems used in business include: management information systems, transaction processing systems, executive support systems, decision support systems, knowledge management systems, office automation systems.

We can distinguish some types of information systems security: physical security, logical security, network security, telecommunication security etc. This paper concerns the aspects of logical security that is access control.

2.1. Access control policy

The main role of access control is to ensure that no unauthorized user will be able to gain access to resources (such as files or directories that may hold information) and be able to copy or modify them. It ensures proper protection for information held within the information system so that no individuals or companies will be able to steal or use it. With the fast progress of technologies the security issue becomes the most important issue when any sensitive data is concerned [1].

There are currently many models of access control that suggest rules of guarding data from unwanted guests that we may choose from. Every company should analyze their needs and choose best suitable model for their needs to ensure safety and confidentiality of sensitive data. It is possible to use a model that

ensures central administration of who can and who can't access system's files, or we may leave those decisions to the owners of files. It can be also possible to choose whether this access rules are to be modified statically or dynamically (e.g. during program execution). Every model has its advantages and disadvantages which is why every company wanting to implement them must firstly attentively research each model and study if it will fit their needs (Fig.1).

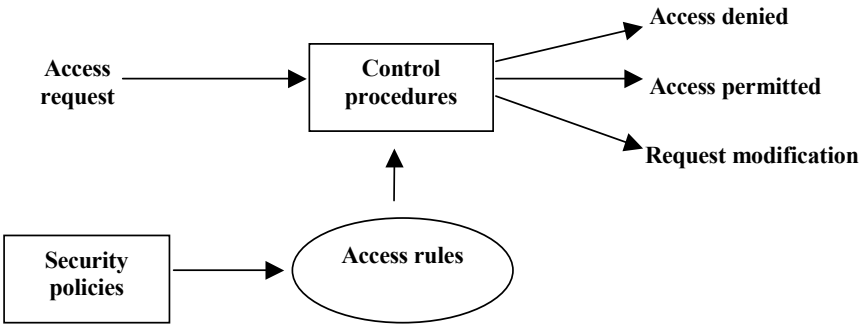

Figure 1. Access control system.
Source: own preparation

Access control models control not only what a user can do or not but they may also control application programs, processes or threads. Some models may also protect metadata – information about processes, users etc. so that for example we cannot find out which users are currently logged into the system [1].

Access control is a process by which users are identified and granted certain privileges to resources, systems or information. Access control components include three main sets: subject, object and operations. Depending on the access control model, these elements can be represented sometimes in different forms.

When subjects gain access to resources depending on their defined privileges they may undertake some actions as for example read the file, modify it or execute it. Therefore privileges (i.e. rights) determine what object user may access and what actions he may perform on it. The main objective of access control is ensuring safety of the objects so that no unauthorized subjects will modify them or use them in any undesirable way.

Access control, apart from granting access to the file itself also provides user authentication, that is ability to verify the identity of users so that they may be held accountable for their actions and ensure what rights and privileges they possess. Authorization may resemble the structure of given organization, it may be based on clearance level of users trying to access an object of given sensitivity level as well as based on lists of users with permissions associated with an object. Among advantages of access control is also easy management of security clear-

ances and tracking history of subjects' actions to make sure we may hold users accountable for them [1].

2.2. Access control models

There are currently many models of access control to choose from. These access models can be divided into two main groups [1,3]:

- *discretionary access control*, where access policies are influenced and modified by the owner of the object and such control over object may be distributed among many users,
- *mandatory (non-discretionary) access control*, where access control policy is enforced absolutely by the system.

It is possible to find many different access control models that can be attached to one of these two groups, e.g. Mandatory Access Control (MAC) model, Discretionary Access Control (DAC) model, Role-Based Access Control (RBAC) model or its extensions.

MAC model is based on decisions made by the system, not by for example owner of the file, who in this model cannot change any access rights. Access control access is determined on basis of object's and subject's sensitivity labels. Every object (i.e. resource) has a label assigned to it in order to determine what level of trust is needed from the subject to grant access. If subject has lower value of sensitivity label he will not get access to given object [1,3]. System has a set of rules determining access policies, but also subjects and objects each have a set of security attributes [1]. Only administrators of the system may pre-define who may access or not given resource. MAC model is used by the military and intelligence agencies to maintain classification policy access restrictions.

DAC model allows access control privileges to be set by individual users. If a user is an owner of a file he may grant or revoke access to it to other users. Each object has an owner that is a user who created the file and thus is allowed to modify its access rights and permissions. Owner may distribute access to given file among many users [1,3]. DAC model uses two types of list in process of rights administration: Access Control List (ACL) – associates permitted action to an object and specifies subjects that can access the object along with their rights to that object, and Capabilities List – attached to a subject and specifies which objects the subject may have access to.

DAC is very flexible and used in commercial and government systems. It is the most widely used model integrated into UNIX and Windows. It enables the users to modify access control to files they own, thus it is more dynamic than MAC [1,2].

RBAC model is used for determining access to objects on the basis of user's role in a system. All the roles have certain sets of rights assigned to them. Roles are assigned to users to authorize them to perform certain operations and actions.

For accessing an object the system requires identification of users roles [2,4]. The main rules governing this model include:

- role assignment – a subject (user) may perform some operation (transaction) only if he has a role assigned,
- role authorization – subjects current role must be authorized to make sure he won't be able to have roles he is not allowed,
- transaction authorization – subject may only execute a transaction if it is authorized for his current role.

This model has many advantages such as flexibility, also the integration of access control for many users into a single role makes management of such system easier and allows more effective evaluation of the access rules.

2.3. Usage control and UCON model

The traditional approach to usage control encompassed three main areas: access control (closed-environment authorization systems that base on identity and attributes of a known user), trust management (authorization for unknown users, based on their properties and capability) and digital rights management (control over the usage of resources that have already been disseminated) [5]. These three components were studied separately and only Usage Control (UCON) approach encompassed all these three elements of logical security.

The UCON concept can be divided taking into consideration its scope. The distinction can be done based on control domain: the system might include a Server-Side Reference Monitor (SRM), where a central entity manages usage control (this approach addresses primarily the issues of access control and trust management), a Client-Side Reference Monitor (CRM), when a client-side application controls access to resources (this approach addresses primarily the issue of DRM), or both [6].

Definition of rights in UCON model is fairly similar to that arising from the traditional approaches: rights are privileges a subject (e.g. user) holds on a certain object (e.g. files the user wants to access), represented by a usage function enabling access to objects [5,6]. The core idea of UCON model is the possibility of detecting certain rights in dynamic way. Certain usage decision functions are applied to determine the existence of a right whenever a subject wishes to access the object. The result of these functions depends on subject's and object's attributes. Also, these attributes can be altered as a result of executing a right, which then can have an influence on future usage decisions (e.g. the user may have the possibility to access a file five times only, or access only one file of a given type). This ensures a fully dynamic approach to usage control [5].

The UCON model consists of three core components, i.e. subjects, objects, and rights, and three additional components that are mainly involved in authorization process, i.e. authorization, conditions, and obligations. Subjects and objects

can have in addition the attributes, i.e. subject attributes and object attributes that define the additional characteristic features of subjects or objects, which can be used in decision process of usage control. An attribute is regarded as a variable with a value assigned to it in each system state (Fig.2).

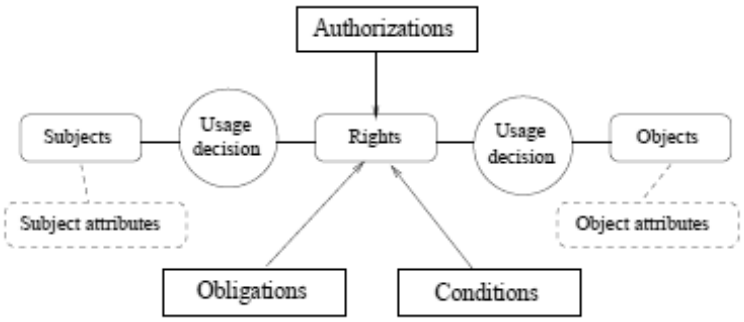

Figure 2. Elements of UCON model.
Source: own preparation basing on [5]

The decision whether to allow a subject to access an object involves testing authorization rules (a set of requirements that must be satisfied before accessing the object), conditions (environment-related feasibility of access), and obligations (the mandatory requirements that a subject has to perform on gaining access to a particular object).

Authorizations are predicates based on subject and/or object attributes, such as role name, security classification or clearance. Obligations are actions that are performed by subjects or by the system before or during an access. For example, playing a licensed music file requires a user to click and see an advertisement, and downloading a white paper requires a user to fill out a special form. Conditions are the system and environmental restrictions, which are required before or during an access, such as system time, user location or system mode.

3. APPLICATION IMPLEMENTING UCON MODEL

The UCON model is an abstract model that represents the usage control approach in security of information systems. It contains the set of logical security concepts that can be used in practice to define the security rules for particular information systems of enterprises. We decided to study how the UCON model can be useful in creation of security schema of an application of information system. The main advantage of this model is the possibility to manage the dynamic aspects of access control in current applications or information systems.

The exemplary application was created to check how the elements and principles of UCON model could be put into practice. This application is a web service offering an online music store. It will allow customers to buy, download and upload music files to the system, putting a price on them, and availing the users with a possibility to buy the credits. The service also allows browsing through the files on offer to find those the users wish to have. The users can have the access to different levels of the application's functionality based on membership type. For this reason, they can be divided upon the level of privileges into three groups:

- *Guests* – new visitors with no account, only allowed to view the content of the webpage restricted to the home page, About page, and the list of music files available,
- *Registered users* - users whose accounts have been activated, potentially eligible to perform certain transactions,
- *Administrator* - the person that has access to all application data via a separate administration area.

Furthermore, the registered users can have different privileges depending on the type of membership. They form two groups: *Regular* and *Premium* users. Regular users are only able to upload, buy and download files, and have to watch advertisements upon downloading. Premium users do not have this limitations and additionally have access to the transaction of trading.

In order to start using the website, user has to be registered and buy sufficient amount of credits. He declares that he wants to buy file from other user. If a person wants to download a file, he or she will often have to watch additional advertisement. Premium user has privileges that can be bought for additional credits.

The basic functionality of the application contains:

- registration of a new user,
- buying of first credits in order to start trading with other site members,
- adding of user's own file to the site,
- buying of selling the tracks – in this case the application browser allows searching by track names,
- editing or deleting of files by a user but only these files of which he/she is the owner,
- each user has his own personal site on which he can see information about number of actual credits, the list of his uploaded files, list of downloaded files, accepted transfers and transfers sent,
- user can buy on the website additional rights (*super user rights*) which allows him to omit the advertisements and waiting for downloading files as well as access the trade operation.

Administrator of the application has the privileges that allow him to change the most important functionality of the website like groups with their privileges, service availability, advertisements, users. He has the additional rights to switch off

and on the website functionality. For example, when updates are being made on the website, the website goes down. There is also another rule that the site goes down at certain hours that have been set earlier.

In addition, before performing a transaction, the user has to agree on the current version of the Terms of Use that covers the aforementioned rules as well as privacy and copyright issues, membership fees. The Terms of Use might change over time.

3.1. Application transactions

It was decided to create separate classes (*transactions*) for each action performed by the user needing authorization, since each action may need different components checked for access permission and different data saved to the database at the end of transaction. The user actions include buying, downloading, editing and removing files, registration, upgrading account and uploading music files for sale.

Interface *Transaction* has basic functions needed for performing access permission actions according to the UCON model – functions for checking authorization, obligations, conditions and finally a commit function that makes permanent changes in database according to type of transaction class. This base class contains also variables *StatusType* that are returned by each function and they can be used to check if the function was executed successfully and allowed access (status will be complete or commit) or not (e.g. rollback, insufficient funds, service unavailable). Through the *status* information it will be possible to inform the user in case of unsuccessful try to gain access what was the exact reason this access was denied.

The *Buy* transaction is responsible for enabling a user to buy a selected music file. User may purchase as many music files as he wants, however he must have enough credits to do so. We must ensure he fulfills all the requirements imposed by access control policies. User may also have already bought the given file and have some available downloads for it left so we must ensure he will use up all the downloads left before attempting to purchase the file again. After fulfilling all the conditions and the purchase the database can be updated with appropriate information that the given user bought a particular music file and modify the users amount of credits accordingly.

Download is responsible for allowing a user to download a music file that he earlier purchased. This action is only available if the user has the file in his bought files list, otherwise he will have to purchase it first. After each download the count of available downloads left for the particular user-music file relation is decreased and updated in the database. If the amount of downloads left reaches zero the user must purchase the file again to be able to further download it.

Edit allows the user to edit information about a music file that he is an owner of. He may edit only the files that he uploaded to the server. He may edit such information as song title, artist name, price and downloads of the file that will be available to those who purchased it.

Register ensures proper registration of a guest user. After registering, the user is assigned to a free Regular user group that will allow him to upload, edit, remove, buy and download files. From this group he will be allowed to upgrade to Premium membership that will allow him to omit advertisements before downloading files (which are obligatory to view for regular users) and trade files with other Premium users.

Remove is a transaction for removing a file, which may be performed only by the owner of the file. After the owner decides to remove his music file it will become unavailable for purchase. However, those users who have bought the file before removal, will still be able to use up their amount of available downloads left since file will remain on the server for some time.

Upload is a transaction for uploading files by the users to the server and allowing them to sell them for a set price. During upload the user specifies the title of the song, its artist and price as well as how many downloads will be available. All the users apart from guests are allowed to upload files to the server. During upload a new music file is created and all its information, along with a link to it is saved to the database.

SendInvitation and *AcceptInvitation* are transactions managing the file exchange. They provide safe exchange operation, investigating such issues as sending to invitations for the same set of files, for a file the user owns etc.

3.2. Implementation as regards UCON components

The created application includes a big amount of authorizations and condition rules as well as a number of obligations examined whenever users wish to access a particular file. These components work in both a static and dynamic way.

The first UCON set of elements is subjects that are represented by users whose properties are collected in the User model. This is an identifiee subject type, as it represents a certain set of credentials. However, it can also represent a provider subject if the User owns a file uploaded onto the server. The concept of consumer rights separated from identifiee rights is not utilized, since any cooperation of the application with a custom player for the files did not been provided, nor any DRM policies did not been introduced to be imposed on the downloaded files.

The model has certain attributes, which can change as a result of executing a certain right. For example the number of credits will be decreased when the user buys a file. Also, the *User*'s group can change once the decision to upgrade to a premium user has been made. The *User* also contains a field indicating whether the most recent terms and conditions introduced have already been agreed on. This

is an example of checking global obligations before any transaction is committed. Some attributes, however, are static, and can only be changed by means of an administrative action (e.g. username and the password).

The *Group* can also be considered as a subject, and it has its own attributes. Those are boolean values, representing the accessibility of certain transaction, as well as a short value, representing the fee users have to pay to become members of a certain group. The default groups are: guests, regular users and premium users. However, when authorization is being checked, we do not rely on the type of the group, but on the group's attributes. These approach is more flexible - if need be, the administrator may define new groups with different transactions accessible and different membership fees. This ensures a finer-grain control over usage policies.

The *MusicFile* should be perceived as an object as far as the UCON model is concerned. It has some static attributes, such as the owner, which can be modified only by the system administrator. In contrast, the attributes as the price, name, artist and the number of the number of available downloads after it is bought can be considered dynamic, since they can be modified by the owner by means of executing modification option, which is also a transaction.

The authorization rules are defined as follows: the primary rule is to check whether the user is not a guest. Unregistered user only has access to viewing the list of files, without the possibility of buying or downloading them. Next, the application checks if the *User*'s group can execute a certain transaction on any file. Then, it is examined whether the *User* has enough credits (in case of buy and upgrade operations) or any downloads left available on the file (in case of download transaction), or whether the *User* is the owner of the file (in case of edit and remove transactions). As we can see, the authorization process relies heavily on subject's attributes, and we utilize the pre-Authorizations UCON variant.

Even before a transaction is started, conditions are tested. The application enables the system administrator to apply a very flexible approach to defining conditions. This will be better understood if we analyze the *ConditionRule* model. The first field of the model defines the type of transaction that this rule will be applicable to. It is possible to set the value of this attribute to ALL, indicating that the rule will be applied to any transaction. The construction of the *ConditionRule* class results in an ability to define rules of the form 'the value of variable a must be in the range between b and c' or 'variable a must contain c', connected into longer predicates using logical operators.

Finally, the obligations the user has before exercising the rights on a file include displaying an advertisement before the download starts. Checking whether the obligation should be applied depends both on subject's and object's attributes: whether to display an advertisement depends on whether an advertisement has been assigned to the file.

4. CONCLUSION

The UCON model is the first model that allows defining of the access control policy not only based on the access request but also it can be evaluated during the access to the information to which we want to control the usage. Created web application utilizes a wide variety of elements derived from the concept of UCON, implemented in both a static and dynamic way. The presented solution provides a general idea on how the abstract model can be employed in a real application.

It seems that the most proper model to support the security of dynamic information systems is the UCON model. In this model the security policy is dynamic because it can change during the information access. The dynamic change of security policy can be translated by the change of the values of subject attributes or object attributes – there are the mutable attributes. The modification of an attribute can be realized before the information access, during the information access or at the end of the access. However, UCON model does not allow to present the complex organisation from the access control point of view and for this reason it should be extended by some new aspects.

REFERENCES

[1] Castano A. and Fugini M. and Martella G. and Samarati P. (1994) *Database Security*, ACM Press, Addison-Wesley.

[2] Sandhu R. S. and Coyne E. J. and Feinstein H. L. and Youman C. E. (1996) *Role-Based Access Control Models*, IEEE Computer, Vol 29, No 2.

[3] Goncalves G. and Poniszewska-Maranda A. (2008) *Role engineering: from design to evaluation of security schemas*, Journal of Systems and Software, Elsevier, Vol. 81.

[4] Poniszewska-Maranda A. and Goncalves G. and Hemery F. (2005) *Representation of extended RBAC model using UML language*, LNCS, Proceedings of SOFSEM 2005.

[5] Park J. and Sandhu R. (2004) *The UCON ABC Usage Control Model*, ACM Transactions on Information and System Security, Vol 7, No 1.

[6] Park J. and Zhang X. and Sandhu R. (2004) *Attribute Mutability in Usage Control*, 18th IFIP WG 11.3 Working Conference on Data and Applications Security, Spain.

THE USE OF WIRELESS MESH NETWORKS IN CONSTRUCTING INDUSTRIAL SYSTEMS OF MONITORING AND FACILITATING MANAGEMENT

Joanna Porter-Sobieraj

Faculty of Mathematics and Information Science, Warsaw University of Technology

Abstract. In the paper the use of wireless networks to create industrial systems for monitoring and facilitating management is presented. Networks connecting devices within a mesh infrastructure are considered and a comparison with classical wired networks is shown. An analysis confirms the great potential, in terms of cost savings and the possibilities of adapting the constructed system, for using mesh networks in such systems.

Keywords: Wireless Networks, Mesh Networks, Industrial Systems Development

1. INTRODUCTION

One of the problems involved in the designing and constructing of teleinformation systems for monitoring and facilitating management – e.g. networks of speed cameras, CCTV, sensors for monitoring infrastructure networks (water pipes, gas, electricity) or measuring the level of traffic – is to ensure the connection between the monitoring devices and the observation centre.

The use of wired networks (optical fiber or copper wire) for this type of system provides a guaranteed quality of connection and certainty of data flow at a specified level. There are, however, two fundamental drawbacks. The cost of installation across open ground is very high, especially in urban areas. The second problem is the lack of mobility of the monitoring devices. In the case of a mistake in the system's initial planning stage, it may render some of the devices completely unusable within the whole system. Thereafter, the correction of their position may prove to be prohibitively expensive.

In the paper a competitive solution is considered – wireless networks connecting devices within a mesh infrastructure. As an example, a design for a system for monitoring construction workers is presented. Cost savings are higher and the possibility of adapting the constructed system is better when using mesh networks in industrial systems.

2. IT SYSTEMS FOR THE SURVEILLANCE OF WORKERS

Two commonly used systems which facilitate the surveillance of workers and automation of some procedures associated with human resources management are work time registration (WTR) and access control (AC) systems.

A WTR system allows for automatic capturing of the times when users enter and exit the object or area under observation. This information is used in calculating the working time of employees. According to the Polish Labor Code, timesheets produced by a WTR system can be a criterion for verifying if an employee fulfils his or her obligations deriving from a contract of employment and can be used as a basis for determining remuneration.

WTR systems are typically used together with AC systems, which enable employers to limit users' access to certain premises, rooms or zones in accordance with their licenses, professional qualifications or their function in a given organization.

WTR and AC systems are, above all, installed in office buildings or in small-scale, closed industrial facility.

2.1. Structure of WTR and AC systems

A WTR system is a simple network consisting of time recorders equipped with magnetic, electronic or proximity card readers. Recorders can be of various types: separate to the event handling the entry and exit of workers, supporting both of these events or allowing the defining of the category of event, such as private or business exits. Often, such a system would additionally be equipped with controlled gateways or turnstiles, forcing the card reader to unlock the way. A single time recorder, which can optionally control a gateway or a turnstile, is called a WTR point.

WTR points are linked to a PC with WTR software, reading the events from a recorder and archiving them. Next, on the basis of these data, the timesheet is produced. Summing up, WTR systems are small distributed systems, consisting of one or a maximum of a few WTR points, that are installed close to each other at the entrances to a building or gateways to an area of an industrial facility.

An AC system is a more complicated system, whose complexity increases with the number of protected areas and the number of inputs to each of them. Each zone is supervised by one driver, which can work independently and control up to a few entrances. The minimum configuration for one entrance consists of a card reader, controlled door lock and a reed switch. An entrance to such a protected zone with such equipment is called an AC point. Additionally, depending on the additional I/O modules, the controller can record and respond to events detected by a set of sensors and operate sirens.

The AC drivers are then connected to form a network, which is linked to a PC with the AC software. This software allows the monitoring of the work of the drivers, updating the database of permissions to the protected zones and reading, archiving and analyzing of the data collected by the drivers.

AC systems installed in office buildings where there are more than a hundred people, used by many organizations, or at industrial sites consisting of many buildings, form a distributed system, that usually contains several dozen nodes (AC drivers). In addition, these systems can be installed in facilities that spread out over large areas.

WTR and AC systems are used in buildings, i.e. in premises in which over many years the layout and – more importantly – the location of the rooms inside do not change. Therefore, it is unlikely that these systems will often need to be redesigned.

To build the network infrastructure connecting the controllers and the computers managing their work, cable systems are used. This follows from the nature of the objects in which they are installed, a low failure of links, a guaranteed constant bit rate and the speed of data transmission between system nodes. Moreover, installation is relatively simple. This is mainly building work and may be done by staff who are not specialists trained in carrying out the installation of industrial automation. All that is needed is a team of construction workers working under the supervision of someone with the appropriate building and electrical licenses for designing and directing work in the field of network and electrical equipment installation. These are the standard qualifications required of engineers working on construction projects.

2.2. WTR and AC systems' communication layer

One of the most widely used standards for the physical layer of the OSI model [1] for data transmission in industrial networks is the EIA-485, more precisely known as RS-4851. This interface allows for the building of a network consisting of up to 32 nodes. The range of this network is about 1200 m. Obtained throughput depends on the distance between the nodes realizing the transmission, and it ranges from 100 kbit/s for a distance of 1200 m to 35 Mbit/s for distances of less than 10 m.

If the distance between nodes exceeds 1200 m or it is necessary to obtain a larger throughput of data for the system, it is possible to use signal amplifiers, also known as repeaters. Repeaters can be connected in series, which can efficiently improve network range, but it should be noted that for each amplifier a power supply has to be provided.

The main advantage of the standard EIA-485 is the acquired high resistance to external electromagnetic interference thanks to the use of differential signaling, and the main disadvantage – the need to make a separate network system specifically

for the WTR and AC systems, which is in practice inaccessible to other distributed control and automation systems, or local area networks.

In modern construction, referred to as intelligent buildings, as early as in the design stage the necessity of preparing fast network infrastructure based on Ethernet (IEEE 802 standard) is taken into account. Systems for intelligent buildings (IB systems) consist of many distributed automation and control systems such as the controllers of elevators, lighting, plumbing, ventilation, air conditioning, heating, or WTR and AC systems. Providing a separate network for each of them would not only be a complicated engineering project, but also economically inefficient.

For the purpose of such projects, in order to integrate the management of all the functions carried out by automation and control systems, several standards have been developed that allow for the unification of protocols of communication with drivers and using the common physical layer (network infrastructure). The frequently used standards are EIB/KNX [2] and BACnet [3, 4]. Both protocols are built on the OSI model and define the possibility of data transport over Ethernet (LAN) and IP networks in the case of remote management of IB systems.

Deciding to use controllers compatible with one of these standards makes it possible to create systems consisting of different vendors' solutions, tailored to customer requirements, and not limited by the installed system itself. However, the primary advantage of this approach is the integration of installation costs and the possibility of using the same infrastructure for both the automation and control IB systems and local area networks.

Currently widely used versions of Ethernet (Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet) offer huge bandwidth with large distances between the nodes. The use of virtual local area network technology (VLAN) and prioritizing the packets already implemented at the MAC layer, guarantees the separation of networks of IB systems and short times for data transmission between the elements of the system, less than 0.1 ms. Additionally, in practice an Ethernet network does not impose any restrictions on the number of nodes, which can reach a level of 2^{48} ($10^{14.4}$). The only limitation here is the cost of the system.

The 10 Gigabit Ethernet standard in the latest version, 10GBASE-T (four pairs of wires in a twisted-pair copper cable), provides 10 Gbit/s connections over distances up to 100 m. If there is a necessity to link more distant parts of a system, an optical fiber, totally resistant to any interference, can be used. The Gigabit Ethernet standard, in version 1000BASE-LX (single-mode fiber), can work over distances of up to 10 km.

In a typical project provided for an intelligent building meant for one hundred to two hundreds employees, the total length of cable and optical fiber used for the Ethernet infrastructure is about 40 km. The cost of implementation can reach over 600,000 PLN. This cost covers only the wiring itself together with building ele-

ments (e.g. hose reels or pipes) and installation, without any specialized network equipment, such as sockets, switches, access points or routers. Including these elements, the total cost can even double, depending on the quality of equipment used and the number of nodes. In return, however, the network infrastructure provides high reliability, high guaranteed bandwidth and guaranteed transfer times of data exchange.

3. MONITORING SYSTEMS IN BUILDING UNDERTAKING

3.1. Problems with establishing work time

A construction can be seen as a place of work. There are three groups interested in any work time registration system – the main contractor, the subcontractors and the construction workers. The construction of the buildings usually lasts over a year and the environment changes constantly. Therefore, standard wire cable monitoring systems, designed for static environments, are very problematical to use.

The main contractor is responsible on the construction site for the safety of the work and all the staff (their own workers and all subcontractors). The contractor has to monitor the amount of staff and location of individual persons and report the working hours of employees to the Building Control and Inspection of Labor. An additional problem is checking if persons performing specialized work have valid licenses, even if they are employees of subcontractors. Otherwise, in the case of the supervision and detection of failures, the main contractor is exposed to financial penalties and, potentially, suspension of construction until the matter is clarified.

Another important aspect is that subcontractors submit to the main contractor reports of the working hours of their personnel, which need to be verified. It should be noticed here, that most of the time the construction site is an open space, without exact divisions such as walls and doors. Such a situation is not well provided for by standard WTR and AC systems. Nevertheless, standard systems, installed near the entrance to the building site, are currently used. They are supported by dedicated staff monitoring the subcontractors. A common solution is for only these chosen people to use WTR cards. When the workers enter the construction site by the main gate, they count them with the help of a WTR system. Next, during the day, the number of personnel and their location are manually checked. Usually, some visual aid supporting the manual counting process, e.g. different colors of shirts for different subcontractors, is used. Unfortunately, workers constantly move around at the construction site (e.g. in search of building equipment), so manual calculation very seldom returns the correct results. The second problem is the common practice of the subcontractors moving their workers to another building site illegally, after they have been counted by the WTR system.

Obviously, there are also opposite situations, when a subcontractor provides a fair work time account, which is in turn questioned erroneously by the main contractor. The lack of a superior, and recognized by both sides, system of worker monitoring does not allow for the authentication of an account. Such a system, preferably – certified and compliant with labor law, would create a reliable reporting document and settle all possible contentious issues.

The third group who are interested in a common monitoring system are the workers themselves. Construction workers are usually poorly educated in labor law and unaware of their rights. Therefore, they are often tricked by their employers via the use of unfair labor accounts, especially regarding overtime and night hours, when a normal day's pay is registered instead of a higher rate of pay.

Summing up, a system monitoring the working hours and building licenses of workers would eliminate a lot financial dangers, and also decrease the risk of accidents. It would also unequivocally solve disputes between the three interest groups specified earlier. In addition, a WTR and AC system certified and specially designed for construction sites, would constitute a reliable tool for the supervisors of the Building Control and Inspection of Labor, facilitating the monitoring and protection of all workers.

3.2. Functionality of the monitoring system

The system for monitoring construction has to register the various events specific to each construction case. As in WTR and AC systems, each worker should be assigned a unique ID token. The information about the worker, relevant to the system, is:

- personal data,
- professional qualifications held and the period of their validity,
- periods of time, when the worker can be present at a construction site; these have to be updated regularly to reflect changes in the schedule,
- the company he/she is working for.

On this basis the following situations should be detected:

- breach of contract and not appearing to work,
- unauthorized leave from the workplace,
- attempts to perform professional duties without valid permission,
- remaining on a construction site after hours, which may be due to an employee accident, or turning up after the working hours, specified in the contract, have passed.

The system should also provide an approximate position for a given worker and watch the location of a chosen group, representing e.g. several workers or one or more subcontractors, which would enable the supervisor to find and reach them easily.

Fulfillment of these requirements would give a construction supervisor a powerful tool to continuously verify the execution of contracts with subcontractors and to detect any irregularities. Reports about the activity of workers would also help in improving work-efficiency, improving safety and reducing costs for the company.

4. IMPLEMENTATION OF WIRELESS NETWORKS

The requirements for the system presented above and the specific work environment exclude traditional i.e. cable-based systems used in WTR and AC systems. The construction site, especially at the beginning, is an open space, without exact divisions such as walls and doors. The site is permanently changing and there is no possibility to install and then adapt the system. In addition, the extra cables would prove disruptive in the typical construction works.

4.1. Wireless personal area networks standards

One solution which perfectly fits the needs of the system is a wireless radio network ZigBee, developed for industrial automation systems. It is based on the IEEE 802.15.4 norm [5], proposed in 2003 and has constantly been improved.

The IEEE 802.15.4 standard describes the physical and media access control layers in the OSI model, introduces a network model with a division of nodes between roles and defines the algorithms and procedures used in radio transactions between the nodes. One of them is the method of locating nodes on the basis of the signal strength received by neighboring nodes of a known position.

The ZigBee specification is an extension of the IEEE 802.15.4 standard. It defines the network and application layers of the OSI model to form a complete protocol for the communication between devices. The ZigBee standard is being developed in order to manufacture low-cost, low-energy, small size and easy to use radio controllers, allowing for the creation of a fully functional network infrastructure for automation and control systems.

ZigBee devices operate on radio frequencies reserved for industrial, scientific and medical purposes (ISM bands). These frequencies are defined in the IEEE 802.15.4 for Europe, USA, Australia, Asia and China. In addition, the standard defines the ability of the system to work on unlicensed worldwide frequency 2.4 GHz. ZigBee radio networks are low-rate wireless personal area networks (LR-WPAN) and, depending on the radio frequency and modulation used, offer bandwidths between nodes of 20 kbit/s, 40 kbit/s, and 250 kbit/s. The range of the radio transmitter is 100 m. These parameters, however, may be extended depending on the radio modules used. Many manufacturers belonging to the ZigBee Alliance offer modules of increased radio parameters. There are transmitters available that

guarantee coverage to 90 m indoors, up to 1.5 km in open terrain and bandwidth of up to 2 Mbit/s when operating at 2.4 GHz frequency.

However, the basic feature of ZigBee networks is the possibility of building wireless mesh networks. The mesh network nodes can communicate not only with each other using a direct radio range, but also relay messages to nodes that are outside of it by using other nodes as intermediate elements, thus forming a multi-hop network. This allows the creation of networks of high reliability by providing multi-path routing, and high throughput by being able to carry out parallel transactions. Such networks can also easily increase their range by adding more nodes to them without having to increase the power of radio transmitters, which significantly increases the operating time of nodes when using battery power.

4.2. Mesh network nodes

The ZigBee specification introduces three types of nodes into the network: coordinators, routers and end devices.

The ZigBee coordinator (ZC) is the master device across the network to which the other devices are attached. Its role is to monitor all the network devices, inter alia, by collecting information about their location – routing paths. This node can also act as the trust center, deciding whether a device can be attached to the network. Successful completion of the new node authentication process ends with the release of a network security key that is used to encrypt all packets transmitted in the network. Without this key, the device will not be understood by other nodes in the network. In the application layer, a coordinator typically serves as the device that collects data from the entire system.

The ZigBee router (ZR) can work as part of the system performing the functions arising from the application, while at the same time acting as an intermediary node in the transmission of packets between devices in the network which are not in direct radio range. Routers also mediate the process of authentication devices joining the network, so these devices can attach to the network at any point. Therefore, direct radio communication with the coordinator is not required.

The ZigBee end devices (ZED) implement the minimum functionality that allows them to communicate only with the parent nodes, routers, or coordinator, but not between themselves. They can also participate in the process of routing, forwarding packets transmitted by other nodes. In most applications, these devices do not initiate data transmission to the coordinator, but respond to requests for cyclical data generated in the so-called polling process. This approach helps to simplify the development of the end devices, at least at the level of the network layer as well as helping to control power consumption by regulating the frequency of queries. In typical applications, the end devices can go into sleep mode between successive data queries.

Devices with full network functionality (FFDs) – routers (ZRs) and the coordinator (ZC) are able to build a mesh-type network, consisting of peer-to-peer network nodes. Devices with reduced network functionality (RFDs) – end devices (ZEDs) – are connected only to parent nodes (ZRs or the ZC) thus forming a star topology subnet (Fig. 1).

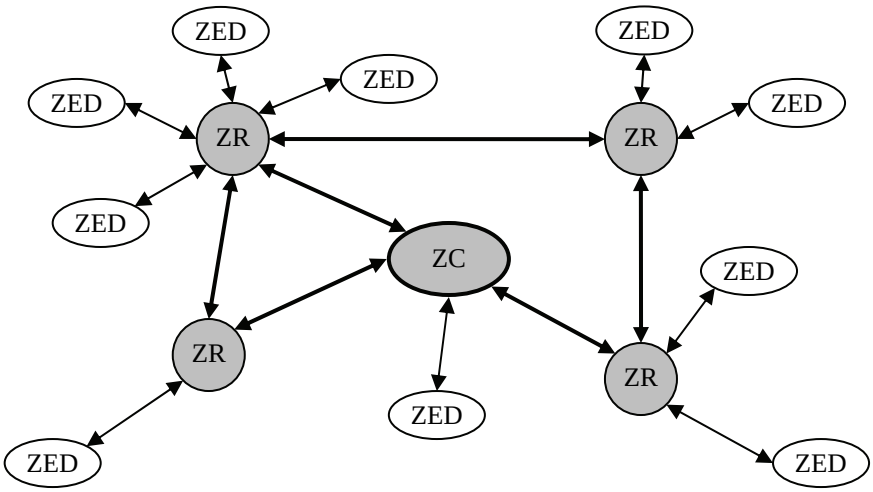

Figure 1. Topology of a network connecting the coordinator (ZC) with routers (ZRs) and end devices (ZEDs) in a system for monitoring construction workers.

4.3. Design of the system

In the design of a system for monitoring construction workers, which is built based on the ZigBee network, end devices (ZED) are ID tokens issued to each worker. These units carry out two functions. One is to join the network using the authentication process performed by the coordinator. This corresponds to the registering of the time of entry into the building in a traditional WTR system.

The second function of tokens is to respond to repeated beacons checking for their presence within the radio range of, either the coordinator, or one of the routers. The interval between the beacons may be adjusted to be between 15.4 ms and 251.6 s. During the time between queries, the devices remain on standby mode. With such a strongly reduced functionality the ID tokens can operate on battery power for a couple of weeks without having to recharge, depending on the frequency of beacon, which is adjustable in the system.

Additional information sent in response to the beacons is the battery status, the signal strength at which the beacon is received and the signal strength with which the answer is given. Information about the status of the battery is used to consider situations, such as when the token has disappeared from the network as a result of discharge, and not as a result of going beyond the range of the system. In addition, supervisors may notify a user to charge the battery or replace the token with another, depending on the procedures in operation. Information about the signal strength, with which the beacon was received and the answer given, is used to determine the distance of a token from the parent device – a router or the coordinator sending the query.

The basic function of a router is to send periodic beacons to tokens. The incoming answers from the tokens are then completed with the value of the strength of the signal received by a router from a given token. In addition, each response is marked with a time stamp, to complete data allowing for the determining of the location of the tokens on the construction site at a specified time.

The routers can work on battery power, as well as on a mains supply, with batteries being recharged during work. Thus, these devices can change their position, depending on e.g. the stage of construction or whether it is possible to install them in a given area. Supervising staff decide on their placement and update the information about the current location in the system to ensure the correct operation of procedures locating a token relative to the position of the router.

The coordinator is a PC with special software installed and connected to a transmitter. It implements two basic functions: registering the tokens in the system and collecting data from routers about the location of tokens. Registering with the network and authenticating tokens involves searching the database for a submitted identifier of the end device and checking its status, i.e. if it is active or not. If this operation is completed successfully (a token is active), then a network security key is sent to the token, used later to correct communication with the routers. The tokens are flagged as inactive if the period, in which the token owner was authorized to access to the site, has lapsed or the date of validity of his or her professional licenses has expired. Each unsuccessful attempt to authenticate is signaled in the monitoring system as an alarm.

The second function of the coordinator – collecting data from routers – consists of receiving information about detected tokens, seeking a list of identifiers that should at a given time be registered with the system (in order to find a given ID), determining the location of tokens based on information sent by routers and recording the history of the locations.

These simple mechanisms in conjunction with the properties of radio mesh networks (ZigBee), provide all the required functionality for the industrial system of monitoring and facilitating management on large construction sites.

5. SUMMARY

The use of wireless radio networks connecting devices within a mesh infrastructure gets rid of the drawbacks of traditional cable systems. The cost of installation is far lower and the ability to adapt the constructed system is significantly higher – from the easy correction of the positioning of nodes to completely rebuilding or installing the system in a different place. Apart from the system for monitoring construction workers presented above, one can easily imagine a system of speed cameras, CCTV or traffic-flow sensors, whose elements can periodically change not only their direction of observation but also location, depending on needs arising from changes that occur in the observed surroundings.

The use of wireless mesh networks, where every node may serve as a transfer point, also allows the use of lower power transceivers. The only condition that must be met is for a radio connection to exist between nodes, which allows the building of a graph in which there exists at least one route between any two of its points. The more disjointed paths between network nodes that can be found, the higher the flow of data arising from the possibility of fragmenting data and transmitting it via different routes.

The downside of radio networks is their sensitivity to interference and their resultant relatively low effective capacity compared to optical fiber or copper wire. However, the considered above mesh structure of links between nodes should solve this problem in practice.

REFERENCES

[1] Zimmermann H. (1980) *OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection*, Communications, IEEE Transactions on Communications, vol. 28, no. 4, 425-432.

[2] ISO/IEC 14543-3 *Information technology. Home electronic system (HES) architecture*.

[3] ISO 16484-5 (2010) *Building automation and control systems. Part 5: Data communication protocol*.

[4] ANSI/ASHRAE Standard 135-2010 (2010) *BACnet - A Data Communication Protocol for Building Automation and Control Networks*.

[5] IEEE Std 802.15.4 (2006) *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*.

ANONYMITY IN E-GOVERNMENT

Damian Rusinek, Bogdan Księżopolski

Department of Computer Scienne, Maria Curie-Sklodowska University, Lublin, Poland

Abstract. E-government, the utilization of the Internet and the world-wide-web for delivering government information and services to the citizens, is already the part of citizens day life, however still many areas of e-government are not commonly used by public authorities. It may be caused by the fact, that they use i.e. sensitive data, which must be secured and protected againts unauthorized. One of main areas of e-government is e-voting, where one of security requirements is anonymity. In this paper we describe a security mechanism that assures anonymity in the world of virtual government. It is an example of simple and easy to implement way that solves the problem of data anonymity in e-voting.

Keywords: E-government, E-voting, Security, Digital signature, Blind signature

1. INTRODUCTION

E-Government may be described with two definitions. The first one describes e-government as the use of computers and electronic devices in order to deliver government services to citizens. When Internet has become world-wide popular, another definition has been introduced. It was described as “The employment of the Internet and the world-wide-web for delivering government information and services to the citizens.” by United Nations in 2006 and “The utilization of IT, ICTs, and other web-based telecommunication technologies to improve and/or enhance on the efficiency and effectiveness of service delivery in the public sector.” [1] by Jeong in 2007.

According to the first definition, the topic of e-government has been started in 1960s. Indeed, the branch of e-government - e-voting – has been started in 1960s when punched card systems debuted [2]. The second definition has been introduced many years later, but nowadays, when Internet is so popular the e-government topic is identified with on-line services.

Internet has brought many advantages to e-government like lower cost, the speedup of offered services, the ease to reach the citizens and many other. However on the other hand e-government in the world of Internet must face all problems that Internet is facing.

The most important and hardest problem in case of e-government is ensuring security requirements. We would like to describe this problem on example of e-voting, which is one of branches of e-government.

2. E-VOTING

E-voting (electronic voting) has similar definition to e-government. The difference is that in case of e-voting public sector services are narrowed to voting services. The general election conducted via the Internet is the typical example of e-voting.

As Bruce Schneier said, e-voting will not replace classic voting in case of the general election until the communication protocol which ensures individual confidentiality and prevents fraud is presented [3].

Therefore, in order to displace classic voting with e-voting we must provide secure communication protocols which ensures the following security requirements:

- anonymity,
- completeness,
- eligibility,
- fairness,
- verification.

In order to ensure listed requirements developers of communication protocols use cryptographic techniques and mechanisms. Introduced solutions are developed in order to create a protocol that may be used for the general election.

There have been some experimental implementation held in order to check if public sector is ready to use e-voting for general election.

The first one was held in USA by California Internet Voting Task Force group. The report has been presented in 2001 and it said that e-voting may be used only as assistant to classic voting until all technical problems are solved.

The second one – Cyber Vote - was held in Europe on request of European Commission. The results were presented in 2003. Project has ended with success, however there was no guarantee that there would be no critical problems when e-voting is used for general election.

There was also experimental implementation held in Geneva in 2003. The project started in 2001, but first elections were held in 2003. Even though the project met with a large wave of criticism, it was considered to be carried out successfully. Project was criticized for not revealing information about software used for elections.

Until now, there is no secure communication protocol and software that could displace classical voting.

3. ANONYMITY

Anonymity is one of the major security requirements not only in e-voting, but also in others e-government services, ie. e-auction. The main problem is to ensure anonymity together with eligibility. It means that protocol must have possibility to check whether voter can vote, but authorities must not associate the vote with the voter who casted it.

In this article we describe a solution to ensure anonymity together with eligibility in e-government communication protocols.

4. DIGITAL SIGNATURES

To obtain eligibility one can use digital signatures. Voter sends his Identity signed with his digital signature. Authorities must check the signature and find the Identity on the eligible voters list. If it is present on the list, voter may proceed to the next step of voting process. The problem is that voter should be anonymous in these steps.

To achieve anonymity in later steps, authorities may use tokens. The idea is that after user's verification, authorities send back one or more tokens that are signed with their digital signature. Voter can use these tokens to prove his eligibility to other instances in later steps of the voting process. The weakness of this solution is that other instances together with authorities may associate tokens with voters. Indeed, authorities may save the association between received Identity and returned tokens. When voter sends his vote, he includes token in the message together with his vote. Therefore, the instance collecting votes may ask authorities for the Identity of the token and associate it with the vote.

To solve the problem of association vote with the identity we describe the solution called Blind Signatures.

5. BLIND SIGNATURES

The Blind Signatures were presented by David Chaum in 1982 [4]. The aim of blind signature is to hide the content of message from the signer without loosing signature.

In the real world it may be compared to the use of envelope and carbonic paper. The sender A needs a document signed by the signer B, but does not want to reveal the content of the document to B. In this case A puts the document into the envelope together with carbonic paper, closes it and gives to B to sign. The signer B cannot open the envelope and check the content of the message. He signs the envelope and the signature is copied onto the document. After returning the message the sender A can open the envelope and take out the signed document.

David Chaum presented blind signatures on example of RSA encryption/decryption algorithm in which encryption security is based on the difficult factorization of large numbers.

In RSA the encryption public key is pair

(e, n), where

n - multiplication of two large prime numbers p and q,
ivarphi(n) - multiplication of $p-1$ and $q-1$,
$e-1 < e <$ *ivarphi*(n) that e and *ivarphi*(n) are coprime,

while the decryption private key is pair

(d, n), where

$$d = e^{-1} \ mod \ ivarphi(n).$$

The difference between using RSA for encryption/decryption and signing/verifying is that for encryption one uses public key and private for decryption while in case of signing the private key is used for signing and public for verifying. Therefore we use (d, n) for signing and (e, n) for verifying.

In case of blind signatures, there is one more step in signing and verifying process included. David Chaums introduces blind factors which play the role of envelope. Blind factors are special numbers that modify the message, so it is not readable and can be removed after signing without loosing signature. The sender A before sending message to the signer B must generate the blind factor as following:

1. A takes B's public key (e_B, n_B),
2. A takes random number r, that r and n_B are coprime,
3. The blind factor is: $r^{e_B} \ mod \ n_B$.

When the blind factor has been generated, A must change the message m :

$$m' = mr^{e_B},$$

and send m' to B.

The signer B cannot retrieve original message m without r and when signing he removes the exponent e_B from r :

$$m'^{d_B} = (mr^{e_B})^{d_B} = m^{d_B} r^{e_B d_B} = m^{d_B} r^1.$$

The signed message $m^{d_B} r$ is sent back to A, who removes r with the inverse r^{-1} :

$$m^{d_B} r \, r^{-1} = m^{d_B}.$$

To sum up, the sender A obtains the signed message m^{d_B} without revealing the content of message m. This cryptographic mechanism is very simple and

helpful, because it solves the problem of ensuring both anonymity and eligibility at once.

In case of e-voting, voter uses blind signatures in authorization phase. He creates authorization tokens on his own and blinds them with authorities' public key. Then, he sends his Identity with blinded tokens to authorities, who check whether he can vote, sign tokens and send them back. Voter removes the blind factor from signed tokens, and from now on he may use them as the proof of eligibility without revealing his Identity. Even in authorities cooperate with other voting instances, they cannot associate voter to his vote without knowing r.

Blind signatures have been widely used in e-voting protocols to achieve anonymous eligibility. In protocols presented in [5] and [6] it has been used as described above. This scheme has been named PVID-Scheme and described in [7].

6. CONCLUSIONS

In this paper authors have described a problem present in some branches of e-government services. It is ensuring anonymity together with eligibility. Not all e-government services need anonymity or anonymity with eligibility, however in case of e-voting or e-auctions it is required. This paper presents a solution for this problem. Described cryptographic mechanism is very simple solution based on RSA algorithm that ensures both eligibility and anonymity at once.

REFERENCES

[1] Jeong Chun Hai @Ibrahim. (2007) *Fundamental of Development Administration,* Selangor: Scholar Press.

[2] Bellis M. *The History of Voting Machines,* About.com.

[3] Schneier B. (1996) *Applied cryptography : protocols, algorithms, and source code in C*, New York: John Wiley & Sons, USA.

[4] Chaum D. (1983) *Blind signatures for untraceable payments*, Proceedings of CRYPTO 82.

[5] Cetinkaya, O., Doganaksoy, A. (2007) *A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network. Availability, Reliability and Security,* ARES 2007.

[6] Rusinek D., Księżopolski B., (2009) *Voter non-repudiation oriented scheme for the medium scale e-voting protocol*, Proceedings of the International Multiconference on Computer Science and Information Technology, Mragowo, Poland.

[7] Cetinkaya, O., Doganaksoy, A. (2007) *Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols*, First Int. Workshop on Advances in Information Security, Vienna, Austria.

EVENT AND PERFORMANCE LOGS IN SYSTEM MANAGEMENT AND EVALUATION

Janusz Sosnowski, Piotr Gawkowski, Krzysztof Cabaj

Institute of Computer Science, Warsaw University of Technology

Abstract. The paper outlines the space of event and performance logs which can be collected in computer systems to support managing and evaluating system operation. We concentrate on methodology of finding anomalies and assessing system dependability or resilience. General considerations are illustrated with more details on storage problems and network attacks.

Keywords: System logs, Performance, Reliability, Dependability evaluation, System administration

1. INTRODUCTION

Contemporary IT systems are becoming more and more complex in hardware and software. Hence various problems may occur due to reliability issues, design faults, configuration inconsistencies, component interactions, external attacks, etc. Detection and diagnosis of these problems is not trivial. This process can be supported by collecting and analysing various event and performance logs.

Most publications devoted to system logs (e.g. [2,9,11] and references) are targeted at system reliability issues (detection and prediction of failures). Moreover, they are limited to some specific systems. We extend this approach for more general problems related to anomalies and system resilience (capability of adapting to changing conditions). The format of registered logs is not uniform and their informative contents is quite often ambiguous [2,9]. We have got some experience in these aspects monitoring many computers used in our Institute (e.g. [11]). This experience allowed us to develop more systematic approach to dealing with two aspects: finding operational profiles of the systems (in different time perspectives: instantaneous behaviour and trends) and identifying anomalies by combining and correlating various logs (covering different resources, their state changes, performance issues, etc.). In particular we consider the problem of selecting the most sensitive monitoring measures related to these aspects. The presented considerations are related to the developed data repository system.

Section 2 presents the scope and goals of system monitoring. Section 3 outlines some specific issues of storage monitoring – crucial point in many systems. Section 4 comments detection of external attacks, section 5 concludes this work.

2. THE SPACE AND GOALS OF SYSTEM MONITORING

Computer systems are instrumented to provide various logs on their operation. These logs comprise huge amounts of data describing the status of system components, operational changes related to initiation or termination of services, configuration modifications, execution errors, security threats, etc. Events are stored in various logs, for example: security, system, application logs, etc. The list of possible events in Windows systems exceeds 10000 [11]. In Unix and Linux systems over 10 sources of events and more priority levels are distinguished.

The formats of registered events have some loosely defined general scope. In particular we can distinguish various data fields comprising specific information in textual or numerical form with some specific brackets, etc. Some fields can be considered as parameters (compare section 4). Usually, at the beginning, we have the time stamp (the time of event registering), name of the event source (e.g. disk, application program, process PID, etc.), text describing the related event problem, severity of the problem. However, events of different classes can be stored in different log files (e.g. security events specifying authorization problems, user login and logout events). The included texts can be very general and of low information value or more specific. Their meaning can be better interpreted after gathering some practical experience within a longer observation time period.

Having checked the capacity of collected logs in some sample computers within the Institute (and some external ones) we can state that the number of registered events is quite high even in systems with low activity. In most cases the system operates correctly, so identifying critical or warning situations is to some extent problematic. Only some events are critical, on the other hand some event sequences or contexts can also be considered as interesting for the further analysis. Targeting at such analysis we should start with identifying different classes or types of events. If we take into account complete event specification than each event is distinct at least within the time stamp field (however, due to limited registration time granularity, the same time stamp is also possible). Having rejected the time stamp field we still notify a large number of different event reports, so some form of more sophisticated categorization is needed. In particular it may be reasonable to eliminate in this categorization argument fields (assuming various value e.g. PID). Moreover, such categorization may be user oriented so it seems reasonable to introduce some flexible mechanism for this purpose e.g. regular expressions, to abstract the events [11]. In the case of Windows it is simpler due to explicit event

ID. Moreover, some time and space filtering can be used to eliminate some redundancy in events.

Another issue is getting long term experience by monitoring event logs for longer periods and on different hardware and software platforms. This monitoring should be correlated with systematic users and administrators' observations, their reports on operation anomalies, occurred system crashes, power blackouts, network disconnections, system overloading or other problems. All these situations should be described and registered in some special repository. This can be confronted with the collected logs at the time of problem appearance or in a postponed log analysis.

In parallel with event logging, various data on performance can be collected in appropriate counters (e.g. provided by Windows, Linux) and according to some sampling policy [4]. These counters are correlated with performance objects such as processor, physical memory, cache, physical or logical disks, network interfaces, server of service programs (e.g. web services), I/O devices, etc. For each object many counters (variables) are defined characterising its operational state, usage, activities, abnormal behaviour, performance properties, etc. Special counters related to developed applications can also be added. These counters provide data useful for evaluating system dependability, predicting threats to undertake appropriate corrective actions, etc. The number of possible performance variables is quite big (many hundreds) and monitoring all of them is too expensive due to the additional load to the system processors and memory [11,13]. Hence, an important issue is to select those variables which can provide the most useful information. This depends upon the goals of monitoring, the sensitivity of variables to the monitored properties of the system, the system usage profile, etc.

Monitoring various objects and selected variables we can identify operational profiles in relevance to different system workloads, operational times, etc. Moreover, they can provide some symptoms of anomalies, errors, etc. The anomaly can be identified by tracing its characteristic properties which differ it from the normal system workload. We can distinguish three classes of anomalies (this is a generalized and extended notion of [1]): i) *point anomalies* – individual measured features or attributes related to system components or the whole system are different from normal values or states; ii) *conditional anomalies* (in [1] called contextual) – the observed features and attributes can be considered as symptoms of anomalies under additional behavioral (not typical) or contextual (related to spatial ant time context) conditions. *Complex anomalies* (in [1] called collective) are specified by multidimensional features (involving combined state of some set of observed measures).

We can look for some statistical deviations (as compared with the normal operation) of the monitored variables e.g.: increase (M+) or decrease (M-) in the mean from the compared reference condition, unimodal left skewed (DUL) or right skewed (DUR), uniform, etc. This approach has been used in identifying 11 cyber-

attacks in [13]. More sophisticated approaches base on finding various correlations between variables, conditioned with events, etc.

Collecting appropriate data within observation window (ΔT_o) allows us to determine that within the time period [ΔT_p, $\Delta T_p + \Delta T_v$] (where ΔT_p - predicted time of problem occurrence starting from the end of the observation period, ΔT_v - time of prediction validity) a problem may appear. Sometimes this prediction can be supported with the probability of problem occurrence. Moreover, the time interval can also be defined in some probabilistic way (fuzzy interval). Some problems can be detected by specific mechanisms almost immediately (low ΔT_o e.g. parity error detection) in a deterministic way. In practice various situations are possible, in particular the problem really can happen in the previewed perspective (CR – correct prediction), beyond this perspective (sooner or later – IP imprecise positive prediction), will not occurs at all (FA – false alarm prediction), will occur despite no detected symptom in the observation time window (SP – skipped prediction or incorrect negative prediction), will not occur and will not be predicted to occur (CN – correct non prediction or true negative). The frequency of these situations defines the quality of the implemented prediction mechanisms. This qualification can be extended with problem attributes (fine granularity prediction). For example predicting faults we can specify their nature: permanent, intermittent, transient.

Searching for system anomalies we can be targeted at some specific problems and correlate them with appropriate events, environment conditions, performance variables, etc. Some of these problems can be obvious (e.g. system failures), others may need some practical experience (e.g. those related to performance issues). Another issue is defining unique and effective symptoms which assure high accuracy and precision of forecasting [14]. One step further is looking for unknown problems, which in fact can be hidden and not harmful at least for some time, however they grow systematically and result in dangerous situations. Looking for such potential threats needs observing many variables in the system, finding their profiles, trends, etc. For example some users may create problems resulting from not sufficient skill in using a new application (this can be identified by comparing operational profiles of many users), cyber-attacks may not cross the introduced firewalls, so we do not feel any harm, but it may be interesting to identify that the system is an object of hackers interest. Correlation of uneven resource or system load, communication traffic may also be attributed to various hidden unknown anomalies.

Analysing performance variables it is important to find mean, maximal, minimal values but also their trends in different time perspectives, distribution in time and amplitude of spike values, distribution of width (burst periods), correlations with other variables, events, etc. Dealing with resiliency we have to check system capabilities of using alternate options, handling additional demands without degradation or loss of functionality, arranging sufficient resources and services in

critical situations (emergencies) or environment changes. Deploying safety procedures, restoring system stability in time, etc., it is worth noting that generated warning signals by many systems (e.g. based on detecting some threshold crossing, specific event) are not accurate and often misleading, so it is reasonable to refine these mechanisms taking into account the experience of system administrators.

3. MONITORING STORAGE SYSTEM

Monitoring storage system covers several administrative aspects. First of all, the user can get the knowledge of current usage profile (e.g. storage capacity in use, read-only data volume, temporary data capacities and accessibility profile), usage trend (e.g. how much storage the company needs in the future? What our demands are – do we need higher performance for read or write, for sequential or for random IO operations, etc.), and finally, the reliability of the system. Among others, the storage reliability is a crucial issue. In [7] authors reported that over 70% of all components failures in large datacenters (more than 100000 servers) are related to the hard disk drive failures. To better understand the "space" of monitoring it is good to be aware of possible failures of the storage system, a heart of which is a set of magnetic hard disk drives organized as RAID (Redundant Array of Independent Disks) arrays for better availability and performance.

One of the important parameter of a hard disk (from the dependability perspective) is the Unrecoverable Error Rate (UER) which defines the rate of possible data loss during disk drive operation. This parameter is assumed to be 10^{14} for desktop-class HDD to 10^{16} bits for the enterprise-class disks. The user may expect the disk operation failure after processing the specified number of bits (i.e. 10^{14} bits is 12.5 terabytes of information). As the disk capacities are growing, using them dramatically decreases the RAID dependability. Assuming five 500GB disks with 10^{14} bits UER in the RAID-5 configuration, there is 20% probability of the second failure during the array rebuild process (array failure). Much better characteristic of enterprise-class HDDs is achieved by manufactures in several ways, both in mechanics and electronics [3, 12], e.g. fully certified magnetic platters against defects with smaller diameters, heavy duty motors with higher speeds, dual processors, error correction and data integrity checks.

Looking closer, the magnetic hard disks are very complicated devices, composed of many high precision mechanical parts, and complicated software (firmware – an erroneous execution of which can provoke the disk failure – e.g. buggy firmware in Seagate's Barracuda 7200.11 disks), and bases on analogue magnetic media. So, the set of possible fault models includes magnetic domain (e.g. platters defects), mechanical (e.g. spindle, heads arm actuators), electronic (e.g. head amplifiers, cache memories, physical interface parts), and software related problems (e.g. bugs in firmware). In fact, a single fault may lead to complex failure scenarios

as mechanical problems may result in magnetic platter damages that may be serious if the vital firmware information is no longer accessible due to the unreadable sector. Some problems are not predictable. However, some of them may be spotted before the catastrophic scenario takes place as their symptoms might slowly arise. For instance, some mechanical problems (with head servo mechanisms, spin engines etc. due to environmental conditions such as dust, humidity, temperature, air pressure, mechanical vibrations etc.) can lead not only to sudden failure but also to some performance degradation. Similarly, the defective sector will be relocated – that also impacts the access time to that sector and is also logged by the disk firmware. In [5] authors report that the disk failure probability is 39x higher within 60 days period after the first scan error. Many other disk operation parameters are also available for the analysis (discussed later on).

It has to be stressed, that due to the complexity of possible defects the early failure prediction or even some error detection is complicated. It can be based on monitoring techniques (section 2). The first idea of disk self-monitoring was introduced in 1992. Recently the SMART (Self-Monitoring, Analysis and Reporting Technology) technique is available in all contemporary disks. The disk firmware monitors a set of attributes related to various aspects. Each attribute (beside its identifier and name) is represented with four values: the current, the worst, the threshold and the raw one. However, the current value is not a direct representation of the attribute's property in most of the attributes. It is rather a calculated value hard to be interpreted directly. The idea is to change the current value (according to some function) – it is assumed that the current value should be higher than the threshold. If it is not true, the BIOS of the computer report the drive to be failing and warn the user. It has to be stressed that attributes reported through the SMART technology and their interpretation can be vendor or even model specific (e.g. different set of attributes, different meaning), and unfortunately, in most of the cases, they are not clearly defined (especially the current and raw values) by the manufactures. That creates problems with building general purpose software to analyze SMART readouts. The goal of the SMART is to prevent from outages/data losses caused by "predictable degradation and/or fault of the device". As some failures have unpredictable nature the user should not be disappointed in such cases. On the other hand, the SMART may warn the user with false alarms. Nevertheless, this technology is definitely not exploited exhaustively. The SMART can be also used as a valuable source of information about the disk to be used in more sophisticated monitoring and analysis systems. Authors in [5] report strong correlation of the disk age (represented in SMART by power-on hours and the number of power cycles) with failure probability. The increase of the operating temperature can originate in ventilation problems (e.g. dust or failure), or reflect the heavy usage of the storage at that time. Higher operating temperatures are reported in [7] as strong failure factor.

It is worth to note that different workloads can impact the failure rate of the HDDs. In [12] authors present that the failure rate of the desktop HDDs can be 2 times higher executing the heavy duty workload. Moreover, it raises another 2x if exposed to the workload based on low-end server pattern. Other important factors relate to the environmental conditions the disk operates in. Among others, they are related to the disk mounting (e.g. firmly mounted with vibration suppression), chassis stability and ventilation. In the enterprise reality this is related to the disk mounting position within the rack and its location within the datacenter [7].

The disk performance reflects in several aspects related to storage management. First of all, the storage performance has to be monitored to keep-up with growing demands of the users and systems it handles, letting purposeful planning of storage infrastructure management. In particular, it also impacts data safety (backup and archiving management, dependability of data carriers, etc.). In the simplest case the storage system can be described with capacity and performance measures (e.g. operations per second, read/write throughput, latency of the requests). Such basic properties are commonly available in the performance monitoring applications built-in the nowadays operating systems. Monitoring them, the administrator should not only take care of the temporary values but also correlate that with different period's perspectives: is the hourly average similar to the yesterdays? Even if they differ, is the profile similar to the one observed a month ago? Or maybe one of the departments is just processing the yearly financial reports – so, the storage usage profile should be correlated with the last year data. As stated in section 2 the analysis should also include the average performance trend. The performance degradation and higher error rates can be used as a one of predicates to suspect failing storage or vibration problems [3], e.g. the access times decreases as the servo mechanism cannot correctly position the magnetic heads (due to mechanical problem or the sector markers are hard to be tracked).

One of the most important conclusions from these observations is that to build more accurate failure prediction model of magnetic disks the one should take into account several sources of information: hard disk built-in SMART attributes (the current value and the historical trend), high level (operating system level) profile of the hard disk usage, and environmental conditions (current, changes and dynamics) – operating temperatures, humidity, vibrations. In the monitored systems we have predicted disk problems in relevance to excessive number of 8219 events (excessive file revealing time) in VSS (Volume Shadow Copy Service) log and excessive initialization time of some applications (performance monitoring).

4. MONITORING NETWORK ATTACKS

As was mentioned in section 2 events and performance logs can be used as well for detection of various attacks directed to the monitored system. Although

many dedicated security systems exists, for example, IDS/IPS (Intrusion Detection System/Intrusion Prevention System), WAF (Web Application Firewall), AV (Anti Virus) and UTM (Unified Threat Management), recent studies show that in many cases appropriate logging mechanism can be used as an additional layer of security. In [8] a report concerning security events in large US computing organization states that only 31% of them are detected by deployed IDS solution and 4% by deployed file integrity checks, which can be treated as simplest host based IDS. In contrast a higher percentage of events (37%) can be detected by analyzing the anomalies in various monitored and logged activities. Additionally, archived history logs are very useful in Forensic Analysis (FA) after detection of the successful attack. This is especially important due to the fact that 27% of attacks are not detected by any layered security (e.g. IDS or file integrity mechanisms) but are reported by external sources. In the sequel we present our experience in detecting network attacks basing on two methods: monitoring some performance parameters (CPU, memory, network traffic) using SNMP (Simple Network Management Protocol) architecture and tracing events collected by Linux syslog demon.

SNMP architecture consists of central Network Management System (NMS) and Agents in various network devices and computers. Each agent manages Management Information Bases (MIBs), which are a description of various parameters that it can monitor. Depending on the system various specialized MIBs are supported. What should be emphasized, NMS can monitor any device or software as soon as its developer provide MIB description in ASN.1 (Abstract Syntax Notation no. 1). On the market there exists many NMS, for example, IBM Tivoli, HP OpenView or even open source OpenNMS. However, a simpler solution can be used. In our research we base on MRTG (Multi Router Traffic Grapher) software. It can be used for data collection and its visualization by plotting any parameter that can be accessed via SNMP protocol. This data is helpful in detecting security relating events.

For an illustration we present and comment some MRTG data collected from a real system in our Institute. This system is used for running multiple virtual machines. One machine is running specially configured SSH server and is used for gathering data concerning SSH scanning and brute force passwords guessing – kind of specialized HoneyPot. Activity of some hackers is so high, that it influences performance of host machine. Fig. 1 presents MRTG statistics during SSH brute force scanning. Some increased value between 6 and 7 o clock is visible on all plots. The duration of this increase (associated with all three parameters) can be a symptom of some kind brute force password guessing. In contrast to this anomaly other spike values relate to some maintenance activity of the system (for example defragmentation of hard drive) and they appear only foe one or two parameters. Such activity can be seen, for example in the first plot as CPU spike, just before two o clock. Further analysis of logs in SSH HoneyPot system confirmed that at-

tacker checks more than 120 passwords. These anomalies can be detected in automatic way. We develop this in the real-time monitoring and reporting system. Similar analysis concerning some suspicious activity of DNS is presented in [10].

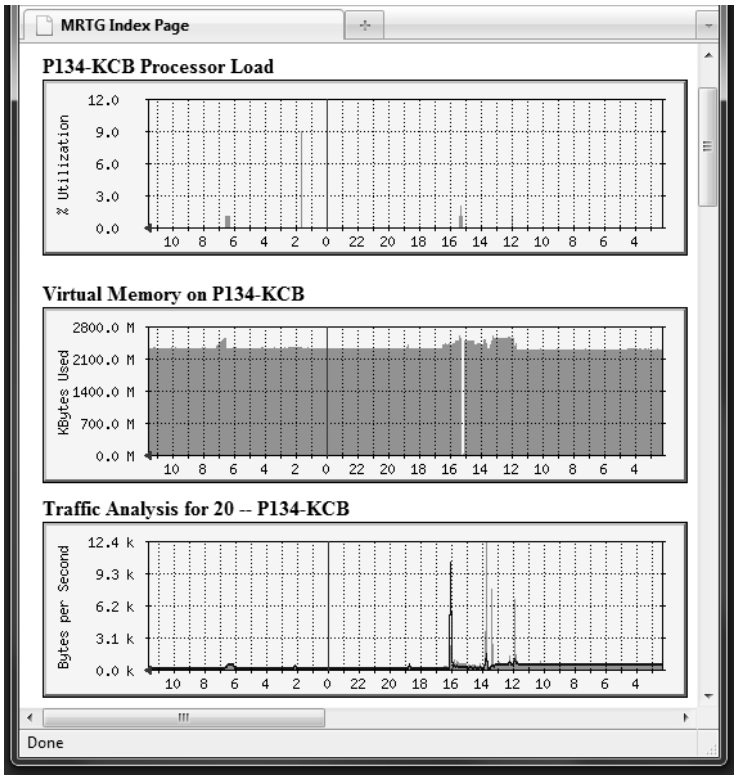

Figure 1. Sample statistics: processor load, used memory, and HoneyPot interface traffic.

The presented analysis based on SNMP and MRTG, can only detect some suspicious activity (in most cases after the actual attack took place). In many cases the attacker activity is discovered after compromising the machine. As an example of event log analysis for security purposes Linux Syslog files can be used. Those logs can be used to determine how the attacker gained the access to this machine.

Syslog is a standard logging protocol in Unix and network devices. Logs generated by applications can be stored locally in the filesystem or sent to a central logging server. Each log has simple header consisting of time and numerical description of this log using two integers – severity and facility. The first number can be used to distinguish level of importance – each log can be marked using some graded labels from critical to debug. The second number (facility) describes the

subsystem that has generated this particular log (e.g. system kernel or a mail service). After the header, the main part of the log comprises some information text.

An example of security related logs is a syslog concerning sshd activity. Two excerpts were logged in the real system connected to the Internet. For security reasons, the real attackers IP address are changed to "aa.bb.cc.dd". In both cases these logs are related to a common method of attack that is a brute force password guessing. In the first excerpt a connection attempt to ssh using various logins is presented (underlined in the presented excerpts). These login names were not available in the given system. The second excerpt shows an attempt to guess the root password. First three attempts are unsuccessful but the last fourth one (underlined) gives the attacker the full access to this machine.

```
May 28 20:38:04 VM sshd[2910]: Illegal user tomcat from aa.bb.cc.dd
May 28 20:38:05 VM sshd[2912]: Illegal user suporte from aa.bb.cc.dd
May 28 20:38:05 VM sshd[2914]: Illegal user oracle from aa.bb.cc.dd
May 28 20:38:06 VM sshd[2916]: Illegal user test from aa.bb.cc.dd
May 28 20:38:07 VM sshd[2918]: Illegal user admin from aa.bb.cc.dd
May 28 20:38:07 VM sshd[2920]: Illegal user prova from aa.bb.cc.dd
May 28 20:38:08 VM sshd[2922]: Illegal user prueba from aa.bb.cc.dd

May 23 19:01:56 VM sshd(pam_unix)[2348]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh rhost= aa.bb.cc.dd user=root
May 23 19:02:09 VM sshd(pam_unix)[2354]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh rhost= aa.bb.cc.dd user=root
May 23 19:02:13 VM sshd(pam_unix)[2356]: authentication failure;
logname= uid=0 euid=0 tty=NODEVssh rhost= aa.bb.cc.dd user=root
May 23 19:02:18 VM sshd(pam_unix)[2358]: session opened for user
root by (uid=0)
```

5. CONCLUSION

The monitoring of various event and performance logs in computer systems is a fundamental source of information on appearing problems or forthcoming threats. Moreover it is useful in load balancing, resource tuning and checking system scalability. The scope and accuracy of monitoring is a challenging issue which can base on long term experience with different systems, collected remarks of system users and administrators, etc. In this process we have also to take into account the assumed goals and system specificity (e.g. workload). In particular it is reasonable to extend the classical approaches targeted at detection of anomalies into forecasting possible problems, finding trends and usage profiles to achieve system resilience.

Further research is planned within log filtering and exploring large sets of logs to identify rules and correlations helpful in the defined monitoring goals.

Acknowledgement. This work has been supported by the National Centre for Research and Development (NCBiR) under Grant No. SP/I/1/77065/10.

REFERENCES

[1] Chandola V., Banerjee A., Kumar V. (2009) *Anomaly detection; a survey*, ACM Computing Surveys, vol. 41, No.3, 15:1-15:45.

[2] Cinque M., et al.,(2009) *A logging approach for effective dependability evaluation of computer systems,* 2nd Int. Conf. on Dependability, 105-110.

[3] Intel, *Enterprise versus Desktop Systems*, http://download.intel.com/support/motherboards/server/sb/enterprise_class_versus_desktop_class_hard_drives_.pdf

[4] John L. K., Eeckhout L. (2006) *Performance evaluation and benchmarking*, CRC, Taylors&Francis.

[5] Pinheiro E., Weber W.-D., Barroso L.A., (2007) *Failure Trends in a Large Disk Drive Population*. Proc. of the 5th USENIX Conf. on File and Storage Technologies.

[6] Salfiner F., Lenk M., Malek M. (2010) *A survey of failure prediction methods*, ACM Computing Surveys, vol. 42, no. 3, March 10.1-10.42.

[7] Sankar S., Shaw M., Vaid K. (2011) *Impact of Temperature on Hard Disk Drive Reliability in Large Datacenters,* IEEE/IFIP Int'l Conf. on Dep. Systems & Networks, 530-537.

[8] Sharma A., Kalbarczyk Z., Barlow J., Iyer R., (2011) *Analysis of Security Data from a Large Computing Organization*, IEEE/IFIP Int'l Conf. on Dep. Systems &Networks, 506-517.

[9] Simache C., Kaaniche M. (2005) *Availability assessment of SunOS/Solaris Unix systems based on syslogd and wtmpx log files; a case study*, IEEE PRDC Conf., 49-56.

[10] Smith D., *Health or Preformance monitoring to detect security events*, http://www.dshield.org/diary.html?storyid=11227

[11] Sosnowski J., Król M. (2010) *Dependability evaluation based on system monitoring.* Al-Dahoud Ali [ed.]: Computational Intelligence and Modern Heuristics (Ed.), Intech, 331-348.

[12] Whittington W., Mastro J., *SATA in the Enterprise*, MS PowerPoint presentation, http://download.microsoft.com/download/9/8/f/98f3fe47-dfc3-4e74-92a3-088782200fe7/twst05005_winhec05.ppt

[13] Ye, N. (2008) *Secure Computer and Network Systems*, John Wiley& Sons, Ltd.

[14] Yu L., Zheng Z., Lan Z., Coghlan S., (2011) *Practical on-line failure prediction for Blue Gene/P: period based vs event-driven*, IEEE Int'l Conf. on Dependable Systems & Networks, PFARM workshop, 259-264.

COMPARISON OF ASYMMETRIC ALGORITHMS USED IN ELECTRONIC SIGNATURES

Tomasz Śmiałowski [a], **Piotr Jałowiecki** [a), b)]

[a)] Warsaw University of Life Sciences
[b)] College of Finance and Management in Siedlce

Abstract. One of the most important factors in development of the modern economy is fast and efficient access to information. State authorities may have a significant impact on the possibility to obtain this access through introducing legal provisions and system solutions affecting improvement of information flow and increase of security during information exchange. The modern economy, often referred to as digital economy or e-economy, is based on fast exchange of electronic information which helps to make decisions immediately and effectively. The present race for customers is primarily a race against time, in which chances of success increase as the areas of using the Internet expand. It is, however, important to effectively ensure security during exchange of information or transactions via the Internet. One of the most important tools to that end is the electronic signature (e-signature). Obviously, it does not work in a vacuum; it is necessary to build an adequate public key infrastructure and establish administrative, economic and legal mechanisms to ensure effective operation and development of the electronic identifier. This paper presents the main issues related to implementation of electronic signatures and compares effectiveness of two well-known encryption algorithms, RSA and ElGamal, that are used for electronic signatures.

Keywords: RSA, EL Gamal, cryptography, asymmetric algorithms, electronic signature

1. INTRODUCTION

The Internet is now the primary channel of communication in the world, acting for some time now as a place, equal to traditional ones, of settling various businesses, administrative and legal matters. However, effective use of the Internet as an environment for commercial and public activity required a possibility of clear, correct and secure identification [6]. The need to have such a tool was the main reason for creating electronic signatures.

An electronic signature is a string of characters (letters, numbers and other keyboard characters) that uniquely binds a document signed and the person signing it. It is characterized by four basic features:

- unambiguous verification of signature authenticity is possible,
- it is impossible to forge a signature,
- the person signing cannot deny or contradict,
- integrity with the signed document.

Two terms are used interchangeably in colloquial speech and often in literature: *electronic signature* and *digital signature*. They represent, however, different notions. Electronic signature is a general term used to identify various electronic identification techniques, including various biometric methods based on human voice, fingerprint, facial shape or DNA, used to exchange information via the Internet or any electronic media. The digital signature is only one of several component categories of the electronic signature. The feature distinguishing the digital signature from other types of electronic signatures is its use. It is based on a pair of keys. One of them, so-called private key, is used to sign electronic documents, while the second, so-called public key is used to verify and confirm authenticity of the received message [9].

According to the Polish law, there are two types of electronic signatures: secure electronic signature so-called qualified signature and ordinary electronic signature [1]. The first one is assigned exclusively to a person signing and is generated with the use of secure tools under the exclusive control of the person signing. It is also attached do the data in such a way that any change of the data is recognizable. An ordinary electronic signature is the data in electronic form attached to electronically transmitted data and used to identify the person signing [2].

Especially the first of these types of electronic signatures has an enormous potential connected with tangible benefits from its use for administration [3], enterprises and individuals. They include: security, operation optimization, reduction of costs and acceleration of information flow [5], [6]. At present e-signature is quickly becoming more and more popular in Poland but one has to notice problems with its implementation and practical application. The most important are: incompatibility (different formats of signatures) and for certification centers – security of software run in MS Windows environment or high cost of HSM devices (*Hardware Security Module*) for official confirmation of receipt. It is also not insignificant that there is a need to create an appropriate public key infrastructure, develop appropriate administrative, economic and legal mechanisms comprising an environment of effective operation of the electronic identifier [4], [11].

The most popular type of electronic signatures is now a digital signature based on symmetric and asymmetric cryptography. Symmetric algorithms, whose operation is based on the same key owned by both the sender and receiver, are

characterized by a greater efficiency than asymmetric algorithms based on two keys: public and private. In terms of security, however, the asymmetric cryptography is much better. This is because in symmetric cryptography the sender and receiver own the shared key which cannot be shared or transferred because it causes a risk of falling into the wrong hands. In asymmetric cryptography this problem was solved in a different way. Private and public keys are created in this case. The private key is available only for the owner and the public key can be sent to persons who verify the signature. If a third party gets the public key, it will result in no serious consequences, because in order to decrypt the information the private key is required. Another advantage of asymmetric cryptography as compared to symmetric cryptography is a relatively small number of keys required (Table 1).

Table 1. Comparison of the number of keys needed when using symmetric and asymmetric cryptography depending on the number of users.

Number of users	Asymmetric cryptography	Symmetric cryptography
1	0	2
4	6	8
10	45	20
25	300	50
100	4,950	200
1,000	499,500	2,000
10,000	49,995,000	20,000

2. PURPOSE AND SCOPE OF STUDY

This paper presents issues related to development of electronic signatures in Poland, as well as the current and projected state of organizational and technical solutions for this area. It focuses on two thematic fields. The first one covers the principles of operation of an electronic signature. The second is a comparison of RSA and ElGamal algorithms in terms of their effectiveness, with a particular emphasis on the analysis of time needed for carrying out fundamental processes: encryption, decryption, generation of signatures and their verification. Moreover, it highlights the main differences between these two popular algorithms of asymmetric cryptography.

3. ASYMMETRIC ALGORITHMS

Development of symmetric cryptography brought more and more complicated ciphers. There are now monoalphabetic and polialphabetic ciphers, multiple-character coding and transposition techniques. In the 60s of the last century IBM began works on a new cryptographic venture, and the result was development of the Lucifer algorithm. Due to increasing requirements, it was subjected to further modifications and, as a consequence, a new standard for data encryption, DES (Data Encryption Standard), was approved in 1977. The IDEA algorithm (International Data Encryption Algorithm) was created on the basis of DES. However, it was a new encryption algorithm that proved to be a breakthrough in cryptography. It was presented for the first time in 1976 by Diffie and Hellman and was based on two keys: public and private. Using this solution anyone can encrypt a message using the public key, but it could only be decrypted by a person with the private key. This eliminated the need of communicating between parties in order to exchange the encoding scheme. This algorithm, named DH from the first letters of its authors' names, was the first asymmetric cryptography algorithm. The main advantage of this scheme is that it is impossible to decode the decryption key using the encryption key and algorithm [13]. Nowadays, the most widely used asymmetric algorithms in electronic signatures are RSA and ElGamal.

The RSA algorithm was developed in 1977 as one of the first algorithms with a private key by Ron Rivest, Adi Shamir and Leonard Adelman, professors at MIT (Massachusetts Institute of Technology). The ElGamal algorithm was created by an Egyptian Taher ElGamal in 1984, on the basis of the original Diffie-Hellman protocol from 1976 [7].

3.1. RSA

Among many public key algorithms proposed so far, the RSA scheme is one of the easiest to implement and use. Many experts highlight its security and it can be ascribed mainly to difficulties in factoring large integers [7], [8]. Originally, the rights to this algorithm were owned by the Public Key Partners, then the RSA Security founded by the creators of the algorithm. This company granted paid licence to use the algorithm in applications from other producers, however, on 6 September 2000 a resignation from the patent rights was announced and the RSA was made public property. The RSA algorithm is embedded in, *inter alia*, the most popular web browsers: Internet Explorer and Netspace Navigator.

It is necessary in the RSA algorithm to generate a pair of keys connected with themselves. The first one is a public key (e, n) used for encryption and verification. The second is a private key (d, n) used for decryption or signing. It is a function of two large prime numbers with a number of digits even up to 300.

The first step to create a pair of keys is to draw two large prime numbers (large prime numbers are considered to consist of 200 to 300 decimal digits), p and q. Because of their crucial impact on the security of a cipher, they should meet *inter alia* the following conditions:

- similar bit-length that prevents factoring based on elliptic curves,
- they should be strong primes,
- difference between them should not be too small because otherwise fast factorization is possible using the trial division ($p \approx q$ or $p \approx \sqrt{n}$).

Factorization, i.e. decomposition into factors, is a process during which for a given x objects are found whose product is equal to x but that are somewhat simpler than x. As a result of a random selection of the first number a problem of primality tests appears. In practice, in order to select the prime numbers, a probabilistic algorithm is used: Miller-Rabin test or Fermat test combined with trial division.

Miller-Rabin test involves drawing the integer a from the interval $1 < a < n - 1$, where n is an odd number and determining the k parameter which defines the accuracy of the test (number of repetitions). It is based on Fermat's test and the method of fast exponentiation and squaring the integer a.

Fermat's primality test is based on drawing the integer a from the interval $1 < a < x - 1$, where x is the tested integer.

$$r = a^{x-1} \bmod_x \tag{1}$$

If $r = 1$ the integer may be prime and if $r \neq 1$, the tested integer must be a composite number.

The trial division uses the small prime numbers (2, 3, 5, 7). The verification covers testing whether a given integer can be divided without remainder by the subsequent numbers within the vector. If it can be divided by at least one of them, the process is interrupted, and the tested number is composite. Then the module n is calculated with the formula:

$$n = p \cdot q \tag{2}$$

The next stage is to randomly select a component of the encryption (public) key e (in practice the value of e is most often 3, 17 and $2^{16}+1$) that satisfies the following conditions: $1 < e < \varphi(n)$, gcd $(e, \varphi(n)) = 1$. The value of $\varphi(n)$ is the value of Euler function calculated with the below formula:

$$\varphi(n) = (p - 1) \cdot (q - 1) \tag{3}$$

After calculating the value of n and e, we designate the component of the decryption key d. It must comply with the following conditions: $1 < d < \varphi(n)$, $e \cdot d = 1 \pmod{\varphi(n)}$.Using the extended Euclidean algorithm, the value d is set. This value is the greatest common divisor for e and $\varphi(n)$.

Transforming the second condition:

$$e \cdot d = 1 \pmod{\varphi(n)} \tag{4}$$

the following formula is obtained:

$$d = e^{-1} \pmod{\varphi(n)} \tag{5}$$

The numbers n and d are relatively prime. P and q used in the process of key generation are no longer needed and it is advisable not to disclose them because it can lead to generation of the private key by an attacker. We assume that w is the information which will be divided into blocks of numbers w_i and s will be the ciphertext - information that has been encrypted (made up of fragments s_i). With this distribution the formula for encryption is obtained:

$$s_i = w_i^e \pmod{n} \tag{6}$$

The numbers s are the encrypted form of the numbers w which are transmitted to the recipient of the information. To decrypt the information we transform blocks s into the original values w. The following formula is used:

$$w_i = s_i^d \pmod{n} \tag{7}$$

Consecutive characters of the text are deciphered from the number w until the full version of the message is obtained.

The RSA algorithm is as follows:

PUBLIC KEY
- n which is the product of p and q
- e which is a relatively prime of $\varphi(n) = (p-1) \cdot (q-1)$

PRIVATE KEY
- $d = e^{-1} \pmod{\varphi(n)}$

ENCRYPTION
- $s_i = w_i^e \pmod{n}$

DECRYPTION
- $w_i = s_i^d \pmod{n}$ [10, 11]

A modified RSA algorithm can be used in electronic signatures. Its modification is very simple and consists only in reversing the encryption and decryption roles. After the key generation process, which is the same as in the case of RSA encryption, one can begin generation of an electronic signature (using a private key), according to the formula below:

$$sig = h(w^d) \pmod{n} \tag{8}$$

where h is a hash function.
The signature created is sent with the message w, because it will be needed during the verification process.

The verification process begins with an initial calculation:

$$h(w) = sig^{e} \pmod{n} \tag{9}$$

After calculating $h(w)$ from the formula (9) and generating $h_1(w)$ independently from the received message w (using the same hash function such as SHA-1) the recipient compares both obtained results. If

$$h(w) = h_1(w) \tag{10}$$

the signature can be tentatively considered authentic.

The RSA algorithm for digital signatures is as follows:

PUBLIC KEY
- n which is the product of p and q
- e which is a relatively prime of $\varphi(n) = (p-1) \cdot (q-1)$

PRIVATE KEY
- $d = e^{-1} \pmod{\varphi(n)}$

SIGNING
- $sig = h(w^d) \pmod{n}$

VERIFICATION
- $h(w) = sig^{e} \pmod{n}$

h - hash function. [7]

3.2. ElGamal

The second commonly used asymmetric algorithm is the ElGamal algorithm. Its security is based on the difficulty of calculating discrete logarithms in a finite field and the Diffie-Hellman problem [10, 14]. This algorithm makes encryption and digital signature possible. Dozens of its modifications (as in the case of the RSA) give us various possibilities. The ElGamal algorithm is not patented, but until 1997 it was hidden under the patent of another asymmetric algorithm - Diffie-Hellman.

The discrete logarithm of the element h (at the base g) in a particular finite group is such an integer x that there is equality in the group:

$$g^x = h. \tag{11}$$

The problem of the discrete logarithm is to calculate x from the following formula:

$$g^x = w \pmod{p}. \tag{12}$$

Just as in the case of the RSA algorithm, the ElGamal algorithm requires a pair of keys associated with each other in order to perform encryption, decryption, signing and verification. The public key (y, g, p) is used for encryption and verification, and the private key (x) is used only for decryption (the RSA private key can encrypt messages) or signing.

In order to generate a pair of keys one should firstly draw a large prime integer p. Then the following values are selected: any generator g of the multiplicative group whose order of magnitude is p ($g < p$) and x which must comply with the following conditions: $1 < x < p$. Then, the value y is calculated with the formula:

$$y = g^x \pmod{p}. \tag{13}$$

After calculating all the components we obtain the public key (y, g, p) that should be available to all users and the private key (x) that should be very well protected. In order to encrypt the message w, one should retrieve the authentic recipient's public key which will be needed in encryption. Then a random number k which is relative prime is selected from the interval: $1 < k < p$. After determining the number k, the parameters a (15) and b (15) are calculated. These parameters are components of the ciphertext sz (a, b):

$$a = g^k \pmod{p}, \tag{14}$$

$$b = y^k \pmod{p}. \tag{15}$$

The ciphertext sz (a, b) is sent to the recipient who will decrypt the original text w on the basis of the sz. The recipient uses their private key in order to do the following.

Calculating $a^{p-1-x} \pmod{p}$:

$$a^{p-1-x} \pmod{\text{p}} = a^{-x} \pmod{\text{p}}. \tag{16}$$

Decrypting the message w with the following formula:

$$w = (a^{-x} \pmod{p}) \cdot b \pmod{p}. \tag{17}$$

The ElGamal encryption algorithm is as follows:

PUBLIC KEY

- p – the prime may be the same for the group of users
- $g < p$
- $y = g^x \pmod{p}$

PRIVATE KEY

- $X < p$

ENCRYPTION

- k – a relative prime from p-1, selected randomly
- a – ciphertext $a = g^x \pmod{p}$
- b – ciphertext $b = wy^k \pmod{p}$

DECRYPTION

- w – plain text $w = (a^{-x} \pmod{p}) \cdot b \pmod{p}$ [10, 11].

A modified ElGamal algorithm can be applied to electronic signatures. Key generation and first steps are the same as for encryption and decryption of a

message with the use of this algorithm. The private key (x) should be used to sign the message w, then one selects a random number k, which is a relative prime from the interval: $1 < k < p$. After determining the number k, a (18) and b (20) will be calculated and will become components of the electronic signature (a, b)

$$a = g^k \pmod{p}. \tag{18}$$

Using the extended Euclidean algorithm a component b is designated. Transforming the following formula:

$$h(w) = (xa + kb) \bmod (p - 1) \tag{19}$$

h - hash function.
We will receive the following:

$$b = k^{-1}\{h(w) - xa\} \bmod (p - 1). \tag{20}$$

The random number k should be kept secret and preferably destroyed because it is generated once again when re-using the ElGamal algorithm. The recipient can tentatively consider the signature authentic after performing verification (21) (in which the public key (y, g, p) is used). Verification should confirmed that:

$$y^a a^b \pmod{p} = g^m \pmod{p}. \tag{21}$$

The ElGamal algorithm for signatures is as follows:

PUBLIC KEY
- p – the prime may be the same for the group of users
- $g < p$
- $y = g^x \pmod{p}$

PRIVATE KEY
- $X < p$

SIGNING
- k – a relative prime from $p - 1$, selected randomly
- a – electronic signature $a = g^x \pmod{p}$
- b – electronic signature $b = k^{-1}\{h(w) - xa\} \bmod (p - 1)$

VERIFICATION
- confirmation of signature compliance, when $y^a a^b \pmod{p} = g^m \pmod{p}$

h – *hash function* [10, 11].

4. RESULTS OF THE STUDY – COMPARISON OF ALGORITHMS

In the RSA algorithm the generated private key can be used both for encryption and decryption and the public key can only be applied to encrypt messages. When it comes to the ElGamal algorithm, the private key is used only to decrypt and the open key - to encrypt the text. The length of the ciphertext in the RSA algorithm depends on the value n - the product of two primes – the ciphertext

cannot be longer than this value. To sum up: the length of the ciphertext in the RSA algorithm is related to the length of the key. In the ElGamal algorithm the ciphertext is always twice longer than the plain text, which makes this method worse in comparison with the RSA. It is characteristic of the ElGamal algorithm that every time it is used, a random number k is generated which results in the same message encrypted every time in a different way. It is the opposite in the RSA: a message is always encrypted in the same way. This is caused by the fact that no random elements are used when encrypting or signing.

The mathematical basis of the RSA algorithm is based on operations on large prime numbers and the basis of the ElGamal algorithm is the discrete logarithm. Computational foundations of both algorithms confirm their security, because up to now no efficient algorithms have been created that in a real time would solve the problem of factorization or discrete logarithm – calculation of x with the below equations:

$$y = g^x \pmod{p}, \tag{22}$$

y, g, p – known values,
x – unknown value to be found,
or fast factorization.

$$a = x * y, \tag{23}$$

a – known values (large prime number),
x, y – unknown values to be found (large prime number).

Both problems, discrete logarithm and factorization, are computationally very difficult to be solved. When it comes to common logarithms and small primes we can manage them with no problem. Currently, it is required that the applied prime numbers should not be shorter than 200 digits. If an algorithm that calculates the discrete logarithm is developed, we will also have an algorithm that will implement factorization of large numbers. This dependence is the reason why the ElGamal algorithm is theoretically not worse than the RSA. The security of both algorithms was proved by their mathematical grounds. This is just one of many aspects of security of these algorithms.

According to many experts, implementation of the RSA algorithm is one of the simplest and most understandable asymmetric algorithms offered. This can also be concluded on the basis of the algorithms described earlier in this work and comparison carried out in this chapter. A feature that points to an advantage of the RSA implementations over the others is the fact that based on the encryption algorithm, when reversing the encryption and decryption, we obtain the RSA signature algorithm. For the ElGamal algorithm, apart from key generation algorithms, both algorithms differ from each other. One should remember about a very important issue: the best algorithm is worth nothing if it is implemented

wrongly from the standpoint of cryptography [12]. The speed of implementation of both algorithms is presented in Table 3 and 4.

The Public Key Partners (later RSA Security) had patent rights to RSA. The company granted paid licences to use the algorithm in applications from other producers, however, on 6 September 2000 the patent expired and a resignation from the patent rights was announced. As a result the RSA was made public property. The ElGamal algorithm had never been patented, but until 29 April 1997 it was hidden under the patent of another asymmetric algorithm - Diffie-Hellman. This way the ElGamal algorithm was the first algorithm with a public key suitable for encryption and digital signatures and was not burdened with any patents. A general comparison of RSA and ElGamal algorithms is presented in Table 2.

Table 3 presents the time needed to implement particular procedures of the RSA algorithm with the use of an 8-bit public key and of the ElGamal algorithm with a 160-bit exponent. Looking at the results one can notice a relationship between encryption and decryption as well as verification and signing. This is caused by modifying the RSA encryption algorithm into the signature algorithm – it consists only in reversing the roles of encryption (which will be accounted for verification in the new model) and decryption (that will implement signing). The RSA encryption requires only one exponentiation of mod n. In order to increase efficiency, the value e (encryption exponent) can be reduced but an exponent that would be too small could lead to a potential attack. Decryption in this system requires also one exponentiation of mod n, but the exponent d (hash exponent) must be no shorter than n. Although both procedures are based on the same mathematical operations, the difference of magnitudes between the encryption and decryption exponents increases the time needed for implementation of decryption. The efficiency of the RSA algorithm for digital signatures (RSA encryption algorithm modification) is analogical. Analyzing the results one can also notice that the time of implementing each function increases with the size of the modulus. The ElGamal encryption scheme requires two exponentiations of mod p: $a = g^x \pmod{p}$, $b = wy^k \pmod{p}$. The RSA encryption requires only one exponentiation of mod n. Exponentiation of mod p in the ElGamal algorithm does not, however, depend on the currently encrypted text. As a result, these calculations can be performed earlier. The result is that encryption is more efficient but the results obtained earlier should be kept secret and stored in a safe place. Decryption using the ElGamal system, as in the case of RSA, requires one exponentiation of mod p. ElGamal signature needs one exponentiation of mod p and calculating $k^{-1} \bmod (p-1)$ with the use of the extended Euclidean algorithm. Similarly to the ElGamal encryption scheme, when generating the signature the above calculations can be made earlier - the results should be kept secret and stored in a safe place. Verification of the ElGamal signature is much more labour intensive than verification of the signature

in the RSA scheme. It is caused by the need to perform as many as three exponentiations. Similarly to the RSA algorithm, we can notice that the time needed to carry out particular functions increases with the size of the modulus.

Table 2. General comparison of algorithms in RSA and ElGamal.

Comparison of RSA and ElGamal		
Algorithm name	*RSA*	*ElGamal*
Computational foundations Security of the algorithm	No fast factorization of large prime numbers	No fast method of calculating the discrete logarithm
Key generation	yes	yes
Encryption and decryption	yes	yes
Signing and verification	yes	yes
Encryption with the private key	yes	no
Length of the ciphertext	Not longer than the value *n*	Twice longer than the plain text
Method of encrypting the same message	Always the same	Different every time
Implementation of signatures based on encryption	yes	no
Patent rights	Not patented since 2000	Not patented since 1997
Implementation	medium	complicated
Date of creation	1977	1984
Speed of the algorithm implementation	Table 3 and 4	
Attempts of breaking	Partially successful (RSA Factoring Challenge)	NO (for large numbers)

Table 3. Time in seconds needed to complete processes of the RSA algorithm for different modulus lengths (with an 8-bit public key) and of the ElGamal algorithm for different modulus lengths (with 160-bit exponent).

Key length	512 bits		786 bits		1024 bits	
Algorithm	RSA	ElGamal	RSA	ElGamal	RSA	ElGamal
Encryption	0.03	0.33	0.05	0.80	0.08	1.09
Decryption	0.16	0.24	0.48	0.58	0.93	0.77
Signing	0.16	0.25	0.52	0.47	0.97	0.63
Verification	0.02	1.37	0.07	5.12	0.08	9.30

Source: Bruce Schneier *Applied Cryptography: Protocols, Algorithms, and Source Code in C*.

Table 4 shows the time needed to complete processes in the RSA and ElGamal algorithms for different key lengths which confirms the results available in the literature (Table 3). However, studies indicate a much smaller time differences in encryption and verification of the ElGamal algorithm.

Table 4. Time in milliseconds required to complete processes in the RSA and ElGamal algorithms for different key lengths.

Key length	1024 bits		2048 bits		4096 bits	
Algorithm	RSA	ElGamal	RSA	ElGamal	RSA	ElGamal
Encryption	3.9	45.3	9.3	343	28.0	2613
Decryption	16.6	21.8	47.3	173.3	349.4	1307.3
Signing	13.1	23.3	47.2	157.9	352.5	1190.3
Verification	2.9	51.6	7.8	361.6	24.8	2691.1

5. CONCLUSIONS

The aim of this study was to compare two most popular schemes used in asymmetric cryptography - RSA and ElGamal algorithms. Therefore, working characteristics of both algorithms were identified and an application was prepared to compare the speed of their operation.

The RSA algorithm is based on the difficulty in factoring large numbers. It was developed in 1977 as one of the first private key algorithms. The ElGamal algorithm, created in 1984, is based on the difficulty of calculating discrete logarithms in a finite field. Since the RSA and ElGamal algorithms are asymmetric, it is possible to generate a pair of keys that are used in the processes of encryption and decryption as well as signing and verification. Computational foundations of both algorithms prove their high security. For the RSA algorithm, the private key generated can be used both for encryption and decryption, while in the ElGamal algorithm the private key is only used for decryption. A characteristic feature of the ElGamal algorithm that every time it is used the message is encrypted in a different way, in the case of RSA it is the opposite. We can obtain the RSA signature scheme on the basis of the RSA encryption algorithm. The encryption and decryption roles should be inverted and in the case of ElGamal algorithm, except for key generation, both algorithms differ from each other. Both algorithms are no longer patented.

It is not obvious which of the above asymmetric algorithms is more efficient because of various functions of the algorithms and areas where they would be used. As for encryption and digital signatures, the RSA algorithm is undoubtedly easier for implementation. The ElGamal algorithm is, however, better when it comes to encryption but the RSA algorithm is unquestionably faster. Commonly used for digital signature, the DSA (Digital Signature Algorithm) is a modified and properly defined version of the ElGamal algorithm. It should also be noted that most public key algorithms are available without any licence fees, this also applies to the RSA and ElGamal algorithms.

REFERENCES

[1] Dfd UNCITRAL Model Law On Electronic Signatures, 2001.
[2] Act of 18 September 2001 on Electronic Signature (Dz. U. 2001, No 130 item 1450).
[3] Marcin Butkiewicz *Internet w instytucjach publicznych. Zagadnienia prawne*, Difin, Warsaw, 2006.
[4] Zenon Bieniek, Joanna Glembin, Franciszek Wołowski *Popis elektroniczny w administracji i zarządzaniu*, Warsaw, 2004.
[5] Sławomira Wronkowska *Podstawowe pojęcia prawa i prawoznawstwa,* Ars boni et aequi, Poznań, 2005.

[6] Ministry of Economy *Podpis elektroniczny - sposób działania, zastosowanie i korzyści*, Warsaw, 2005.
[7] Alfred Menezes, Paul van Oorshot, Scott Vanstone *Handbook of Applied Cryptography*, Fifth Edition.
[8] Ron Rivest, Adi Shamir, Leonard Adelman *A method of obtaining digital signatures and public-key cryptosystems,* 1978.
[9] Wiesław Paluszyński *Vademecum podpisu elektronicznego*, Centre for Information Technology Promotion, Warsaw, 2002.
[10] Douglas R. Stinson *Cryptography Theory and Practice*, Second Edition, CRC Press, Inc., 2002.
[11] Mirosław Kutyłowski, Willy-B. Strothmann *Kryptografia – Teoria i praktyka zabezpieczenia systemów komputerowych*, Second Edition, Read Me publishing house, Warsaw, 1999.
[12] Reinhard Wobst *Kryptografia. Budowanie i łamanie zabezpieczeń*, RM publishing house, Warsaw, 2002.
[13] Janusz Stokłosa, Tomasz Bliski, Tadeusz Pankowski *Bezpieczeństwo danych w systemach informatycznych*, Polish Scientific Publishers PWN, Warsaw; Poznań, 2001.
[14] Bruce Schneier *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Second edition, Polish version translated by Roman Rykaczewski, Wydawnictwo Naukowo-Techniczne, Warsaw, 2002.

IDENTIFICATION OF THE STATE OF DECREE DECISIONS FOR INTELLIGENT MANAGEMENT SYSTEMS

Jerzy Tchórzewski

Department of Artificial Intelligence, Institute of Computer Science,
Siedlce University of Natural Sciences and Humanities (UPH)

Abstract. There is a need to define the decrement decision for intelligent management systems. The work undertakes this new research direction - the identification of decision attribution to obtain the model, which is then studied using the example of contractual data for decision making in the tax administration. First, the author discusses intelligent management systems including decrement decision, and then proposes a model managed by the Office electronic decrement decisions, including decisions in the circulation system. Identification of the decrement decision was conducted in the MATLAB environment using the System Identification Toolbox. In the numerical example, 1425 records of data were used that characterize a document which is subject to decrement decision in tax proceedings. Also, the author formulated proposals, including the attempt to define the decrement decision as part of intelligent management systems.

Keywords: Decrement Decision, eOffice, Identification, Intelligent Management Systems, MATLAB Environment

1. INTRODUCTION

A need to define the concept of decrement decisions for intelligent management systems is becoming increasingly urgent. The work undertakes this new research direction connected with the identification of decrement decisions state in order to obtain a model, and then perform research using sample data on decision-making in a government office [2, 4, 6, 10,13, 16-18]. First, IT management systems were discussed paying attention to decrement decisions, and then a hybrid model of the eOffice [1, 3, 5, 12, 15, 18] managed using e-decrement decisions, including circulation of decisions in the IT system, was proposed. Results of research as regards identification of decrement decisions state obtained in the MATLAB environment using the System Identification Toolbox were presented [7, 11, 17, 20]. 1425 records containing data characterizing a document described by the information and decrement decision made in connection with tax procedure were used in the identification process [16-17]. Conclusions were formulated and an

attempt was made to define a decrement decision as an element of intelligent management systems.

2. DOCUMENTS

The word decree exists in legal language, and is defined as a rule of law issued as per act, in extra-parliamentary mode by the President or the Prime Minister, as a normative act issued by an executive power body. The word decrement, defined as a handwritten note on a document, including the method of handling affairs or a resolution recommending making a specific decision, is derived from the term decree. In accountancy, the word decrement is used to qualify documents to be entered in the books of account by indicating a method of entering the document in the books of account, accompanied by the signature of the person responsible for the qualification. In management, managers use decrement as a way of issuing official orders to their employees to handle affairs, and employees also use decrements both intended for their co-workers and their managers as a proof of the state of affair handling.

2.1. Types of decrement

At present there are three types of decrement: management (information and decision-related), financial (income and cost-related) and executory (energy and material-related) [8, 14, 17].

Management decrement - applies to documents related to collecting information on incurred costs including final decision made by the manager of the organization, as well as controlling and supervising documents including the possibility to inspect registered operations.

Financial decrement - applies to the description of documents as regards incurred costs and derived income, including simultaneous entering of the operation in the information system (e.g. FK system), according to the binding law, including tax and balance sheet law in accordance with the decision made by the manager in the form of management decrement.

Executory (realization-related) decrement - applies to the description of documents as regards supply and operation-related aspect of economic events (supplying the organization with necessary energy and material-related streams e.g. energy, raw materials, and half-finished products, machines, human resources, etc., and the obtainable product, service, etc.).

It is also possible to speak about auto-decrement, i.e. a feedback decrement. A special case of such decrement are system's internal decrements. For instance, an internal decrement may be related to a note about costs according to the source of generation, income according to the adopted classification, considering the cost of goods, products or services, etc. sold.

3. DECREMENT DECISIONS IN THE INFORMATION TECHNOLOGY AGE

An obvious consequence of present tendencies in the development of Information Technology is electronization of decrement decisions, including decrement decisions used in finance management [2, 16-17]. So far, the main aim of accountancy in state and economic administration was inventorying administrative and economic events in the financial aspect in order to provide information for budgetary, tax and financial reporting, etc., including information on realized revenue and expenses, income and expenditures, or profits, costs, losses, etc. at the time the report was drawn up.

Implementation of controlling and budgeting, i.e. management accounting principles in an organization entails involvement of organisational unit managers in the process of making financial decisions concerning costs and revenue. From the moment of implementation of management accountancy, the manager makes financial decisions connected with the approval and assignment of costs to the tasks being realized, and consequently is responsible for the results in the area of business activity, which is now under his supervision.

It is possible to assess efficiency and security of a company or an office by assessing individual areas of business activity and the quality of managing these areas by managers as regards the following aspects: organizational, technological, information and decision-related, financial, etc., which is connected with the need to introduce new information systems using electronic methods of information circulation, decision-support systems, making analyses, etc.

For the above mentioned reasons, technological and organizational changes require the introduction of a new quality of *Information Management Systems,* i.e. systems supported by artificial intelligence methods, such as artificial neural networks, evolutionary algorithms, expert systems, immune algorithms, ant algorithms, etc. called *Intelligent Management systems* [3, 5, 17]. To this end, *Electronic Office (Mailroom)* as a place, in which incoming documents are registered, scanned and made available for the purpose of decrement is sectioned off the structure of the organizational unit, enterprise, entity, etc. The next step is the organization of appropriate circulation of documents incoming to every system, their immediate registration in the information system, which ensures control the state of affair handling at any time, and allows managers of organizational units to control the process of making decisions connected with management, administration, substantive law, etc.

Such a formalization is in turn connected with the necessity to introduce a system for registration of affairs to be handled by the government or economic administration, which should be uniform, from the point of view of both the decrement itself and the approval of proposed solutions at individual stages of handling affairs, including possible entering of documents connected with the cost of administrative or economic operation. Registration office becomes a kind of mirror

in which a current situation of the office, administration or company is reflected. Introduction of electronic decrements rules allows to save costs connected with the circulation of documents, passing documents from one employee to another, to improve analysis of documents. It also allows for automatic description, which, leads to financial decrement of economic operations on managerial accounts, etc.

In order to optimize the circulation of decrement documents accompanying standard (base) documents relating to substantive and procedural law, it is recommended to minimize the circulation of unnecessary decisions and give coherence to the circulation of documents including with the accompanying decrement decisions. Here, *Electronic Book of Decrements,* which allows to maintain a specific register of history for each document, is introduced along with *Electronic Book of Documents.*

In this way, on the basis of source documents entered in the system and common for both books, it is possible to obtain verifiable results, regardless of different interpretations resulting from different needs and requirements both systems for document registration must meet.

Intelligent Management System (*IT-System*) may use the company's organizational and IT resources available, as well the existing functionality of the system including the state of preparation and making decrements for documents for the purpose of analyses preceding decision-making, i.e. introducing a new kind of decrement-related activity, which may be called preliminary (initial) decrement.

4. MAKING DECREMENT DECISIONS

The most important thing in making decisions in a government office or an economic office is making choices in compliance with the rules and regulations of law, or with the concluded agreements. Making the right decision requires vast knowledge and professional experience from the decision-maker [10, 13-14, 17-18]. It especially applies to strategic decision-making. In order to avoid making wrong decisions, thorough analysis based on the obtained information should be performed prior to making a decision. The quality of the decrement decision as well as the quality of the resulting factual decision depend on the precision of and accuracy of knowledge acquisition.

Information used in decision-making processes are called *control information* or *decrement information*. Procedures and algorithms supporting making decrement decisions used in decision-making practice determine the range and accuracy of necessary decrement information. Pieces of information significant in administration practice include information on making similar decisions in the past, related to similar substantive law, or information concerning realization. For these reasons, initial (preliminary) circulation of information connected with so called "*matters to handle"* is connected with the retrieval of historic information and legal

interpretations as regards the decisions being made. And it is at the stage of the circulation of the "*matter"* that decrement decisions are made.

In currently binding organizational schema e.g. related to the functioning of government offices, the circulation of electronic documents (*eDocuments*[1]) is based on the office instruction which may be characterized in the following way [4, 8, 16-17]: documents are received by the office mailroom (a specific receptor of the system, owned by the *e-Office*), from where it is delivered to the Secretariat of the Office Head, then the Head adds decrements to documents by passing the matter to the Vice-head, Managers, etc., and finally to employees in various organizational units, who handle the matter [2, 16]. Currently, only part of documents received by the Office are in the electronic form. Most of them are paper documents. The situation in which the system cooperates with the environment (economy, society, administration, etc.) is presented in the diagram in fig. 1 after Józef Konieczny [8].

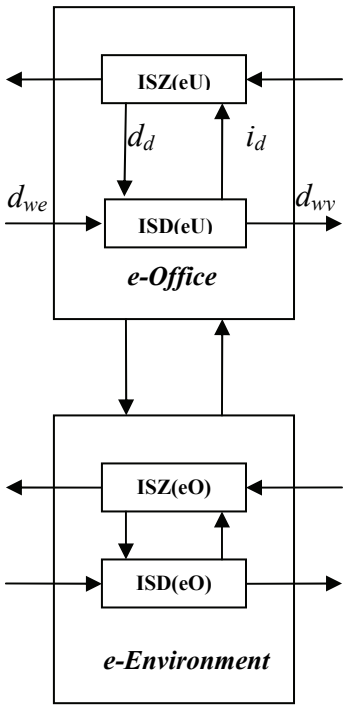

Figure 1. Decision-making process in *e-Office*. Symbols: *PSZ* – paper (traditional) management system, *SW* – executory system, d_{we} – incoming documents, d_{wy} – outgoing documents, i_d – decrement information, d_d – decrement decisions.
Source: author's own compilation

[1] The program *ePoland (polish: ePolska)* introduced in an orderly fashion terminology related to the information society

At present, a diagram illustrating circulation of documents in *e-Office* differs from the circulation of document in *paper-Office* in respect of infrastructure connected with circulation of documents, including the place and form of inflow and outflow of documents as well as the method of processing and circulation. Electronic documents inflow to the I*nformation Management System (ISZ)*, usually managed by the system administrator, they do not inflow to the executory system (SW) - Office mailroom, as in case of paper documents circulation. Moreover, at present, hybrid circulation may occur, with double circulation of documents both in paper and electronic form. In such a case, we may speak about electronic circulation of decrement decisions concerning both processing documents in both paper and electronic form. Some electronic systems dedicated to organizations and offices such as the *KasNet* system, though they are not called hybrid system function in this way.

Due to the fact that decrement decision d_d depends on information connected with the management and executory system, the definition of the decrement decision of the hybrid system may be brought down to the system situation presented in fig. 2. Electronic information concerning decrement decisions and electronic knowledge connected with decision-making inflow to the *Information Management System* functioning in the office [1-3, 5, 16-17]. Making decrement decisions (d_d) of two types: internal and external is influenced by the following: i_k – decrement information, d_{k-i} - past decrement decisions (made at time t-i), d_n – legal norms (acts, regulations, dispositions, etc.), d_{ki} – decisions made by managers at ith level of competence, i_a – analytical information (results of studies and analyses), which may be expressed as follows:

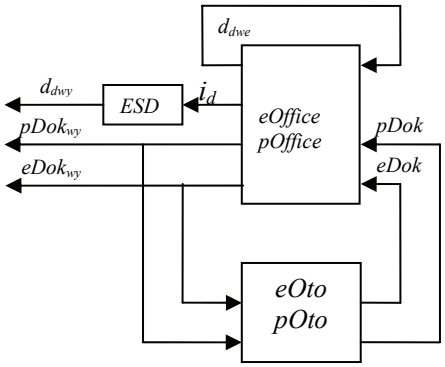

Figure 2. A framework circulation of electronic and paper documents as well as decrement decisions and information in a hybrid office (*eOffice* and *pOffice*). Symbols: {$pDok_{we}$, $eDok_{we}$} – paper and electronic incoming documents, {$pDok_{wy}$, $eDok_{wy}$} – paper and electronic outgoing documents, i_{wy} – outgoing documents, i_d – decrement information, d_d – decrement decisions, *eOffice* – electronic office, *pOffice* – paper office, *eOto* – electronic environment, *pOto* – paper environment. Source: author's own compilation

$$\{d_{dwe}, d_{dwy}\} = \langle d_{k-i} \quad d_n \quad d_{ki} \quad i_k \quad i_a \rangle \tag{1}$$

Table 1 presents characteristic features connected with the above mentioned streams that influence decrement decisions.

5. IDENTIFICATION EXPERIMENT

5.1. Th model of decrement decision

In order to perform the identification of the state of decrement decisions for a government office, it is necessary to obtain appropriately prepared numeric data. In the practical experiment, described in detail in work [7, 11, 16, 17, 20], a set of measurement data contained 7 inputs and one output. Inputs were labelled appropriately: n_{ka} - mailroom number, n_{do}- document name, d_{do}- document date, n_{ad} - sender, d_{wp} - date received, d_{de} - decrement date, o_{do}- description of document.

Table 1. Organizational streams determining the state of the decrement decision that has been made d_d. Source: author's own compilation

d_d	d_{k-i}	d_n	d_{ki}	i_k	i_a	t
d_{dwy}	Decisions made in a similar case as the case being decided in a given process in relation to external entities	International, domestic and regional legal norms, etc. (European law, ordinances, dispositions, etc.)	Decisions made by each participant of the decision-making process (starting with employees preparing a project of solution of the matter, through managers of different levels, to the final decision-maker	Decrement information obtained during preparation of a project of an outgoing decision or document	Information obtained in the process of studies or research on improvement of organization, etc.	time resulting from legal norms, contracts, agreements, etc.
d_{dwe}	Decisions made in a similar case as the case being decided in a given process in relation to external entities	Internal legal norms (statutes, regulations, decisions, procedures, etc.)	Decisions or information concerning results of internal meetings, etc.	Decrement information as memos, superiors orders, notes concerning work managers related to the preparation of material, etc.	Information prepared for the purpose of making right internal decisions by the team of employees, external companies.	Time specified by the superiors as regards their subordinates

However, the output of a system, labelled as zad_{Na} was a department in the office, to which the document was intended for in decrement. Data for analyses were collected in a file named *dane_umowne.xls*[2], which consisted of 1.425 records. Identification data concerned real conventional matters in one of the offices in the Mazowieckie province, which were distorted using an appropriate noise algorithm (fig.3).

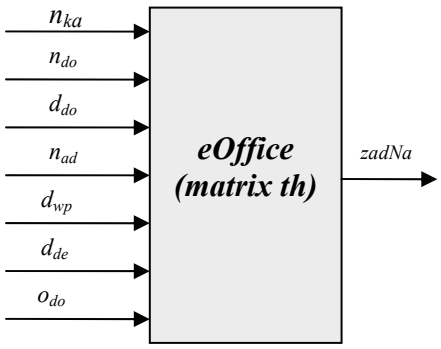

Figure 3. Input and output data in the process of making decrement decisions in a hybrid government office. Symbols in the text.
Source: Author's own compilation based on [16]

As a result of the identification performed in the MATLAB environment using the System Identification Toolbox a model of the process of decrement decision-making (arx) was obtained in the current, functioning, hybrid office (in the office undergoing transformation from the *paper Office* to the *electronic Office):*

$$A(q) \cdot y(t) = B(q) \cdot u(t) + e(t), \tag{2}$$

where:

$A(q)$ = 1 - 0.1532 q^–1,
$B1(q)$ = 0.0006395 q^–7,
$B2(q)$ = 0.04046 q^–7,
$B3(q)$ = 7.02e–005 q^–7,
$B4(q)$ = 7.02e–005 q^–7,
$B5(q)$ = 7.02e–005 q^–7,
$B6(q)$ = 7.02e–005 q^–7,
$B7(q)$ = 0.0555 q^–7.

[2] Source: Szczepanik H. [16]

Th characteristics of the obtained model of the system of making decrement decisions was in the form of arx117 (accuracy 62.3472%), which was presented in fig. 4. Although the accuracy of the characteristics does not exceed 70%, which would be a good result in the identification process of this type, the obtained result may be considered satisfactory because of the fact that the growing tendency is maintained.

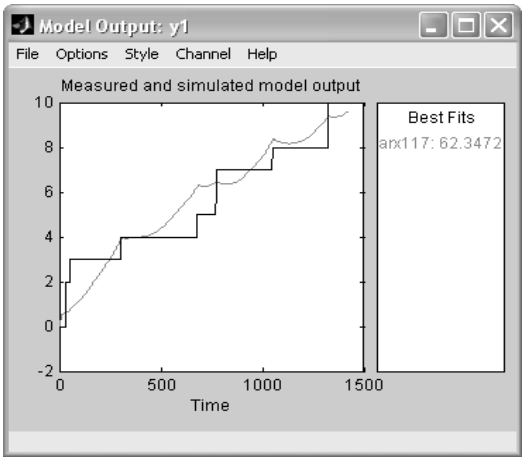

Figure 4. Characteristics of the obtained model of the system of decrement decision-making in a government office (model arx117).
Sourse: Szczepaniak H. [16]

5.2. Model of decrement decision in state space

From matrix *th* (model arx117) it is possible to obtain next model in state space, namely:

$$[\mathbf{A, B, C, D}] = \text{th2ss(th)}, \tag{3}$$

where **A, B, C, D** – matrix, which have next value:

$$\mathbf{A} = \begin{bmatrix} 0{,}15324 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{4}$$

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0{,}000639 & 0{,}040405 & 0{,}000007 & 0{,}000007 & 0{,}000007 & 0{,}000007 & 0{,}055504 \end{bmatrix}, \quad (5)$$

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad (6)$$

$$\mathbf{D} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad (7)$$

In this way it is possible obtain next model in state space:

$$\begin{aligned} \dot{x}_1 &= 0{,}15324 \cdot x_1 + x_2 \\ \dot{x}_2 &= x_3 \\ \dot{x}_3 &= x_4 \\ \dot{x}_4 &= x_5 \\ \dot{x}_5 &= x_6 \\ \dot{x}_6 &= x_7 \\ \dot{x}_7 &= 0{,}000639 \cdot u_1 + 0.040405 \cdot u_2 + 0{,}000007 \cdot u_3 + 0{,}000007 \cdot u_4 + \\ &\quad + 0{,}000007 \cdot u_5 + 0{,}000007 \cdot u_6 + 0{,}055505 \cdot u_7, \end{aligned} \quad (8)$$

$$y_1 = x_1 + u_5 \quad (9)$$

In the result we can have flowchart as in fig. 5.

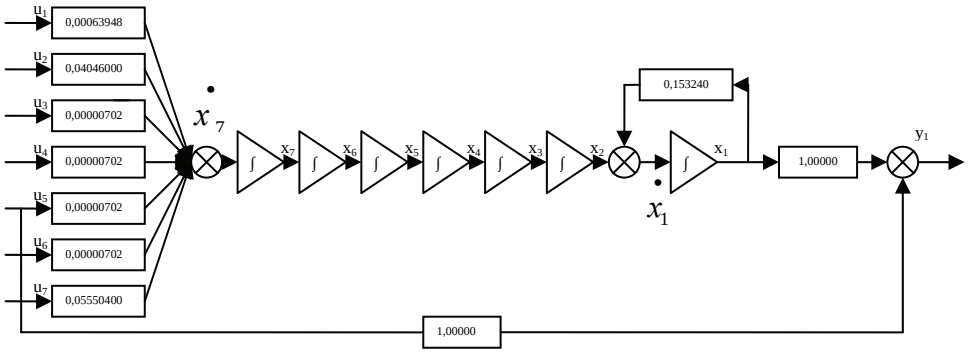

Figure 5. Flowchart of the system of decrement decision-making in a government office (model ss, equation: (8)-(9)).
Sourse: author's own compilation

6. CONCLUSION

The author proposes a new conception connected with making decrement decisions in a hybrid office, prepared from the point of view of possibility to use it in the process of design of intelligent management systems. In addition to the conception of decrement decision itself and its definition, results of research on functioning of the system of making decrement decisions were presented and a model of the system of decrement decisions, which was obtained as a result of identification of a real state office, using the example in which there were 7 input quantities and one output quantity, was presented

Both the conception and the definition of decrement decision can be further improved and new models of systems can be developed based on it.

REFERENCES

[1] Barczak A.: *Designing of hybrid information systems*. IV Krajowa Konferencja Naukowa nt. „*Sztuczna Inteligencja*" SzI 15'2000 AP – PTC –WAT. Siedlce 1999.

[2] Barczak A.: *Informatyka i Telekomunikacja w nowoczesnym biurze*. PWE, Warszawa 1998.

[3] Barczak A.: *Projektowanie inteligentnych systemów informatycznych.* Materiały XI Ogólnopolskiego Konwersatorium nt. „Sztuczna inteligencja - jej nowe oblicze" (badanie – zastosowanie - rozwój) AI-14' 99. AP. Siedlce 1999.

[4] *ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego Polsce na lata 2001-2006*. Ministerstwo Łączności 2001.

[5] Florek J., Barczak A.: Procesy informacyjno-decyzyjne w eksploatacji obiektów technicznych. Instytut Łączności, Warszawa 2004.

[6] Grudzewski W.M., Hajduk I.K.: *Metody projektowania systemów zarządzania*., Delfin, Warszawa 2004.

[7] Janiszewski K.: *Identyfikacja modeli parametrycznych w przykładach*, Akademicka Oficyna Wydawnicza EXIT, 2002.

[8] Konieczny J.: *Inżynieria systemów działania*. WNT. Warszawa 1983.

[9] Kłopotek M.: *Kierunki rozwoju systemów komputerowego wspomagania odkryć*. Instytut Podstaw Informatyki Polskiej Akademii Nauk. Materiały XI Ogólnopolskiego Konwersatorium nt. „Sztuczna inteligencja -jej nowe oblicze" (badanie – zastosowanie - rozwój). AI-14' 99. AP. Siedlce 1999.

[10] Łukasiewicz J.: *Przykłady i zadania z podstaw teorii decyzji*. WUW, Wrocław 2002.

[11] Maślanka M.: *Identyfikacja systemów dynamicznych na przykładzie prostego obwodu elektrycznego*. Archiwum Process Control Club (*http://pcc.imir.agh.edu.pl*), 2001.

[12] Michalski A.: *Wykorzystanie technologii i systemów informatycznych w procesach decyzyjnych*. Wydawnictwo Politechniki Śląskiej, Gliwice 2002.

[13] Nahorski Z.: *Metody i środki wspomagania procesów decyzyjnych*. WNT, Warszawa 1994.

[14] Partyka M.A.: *Logika wielowartościowych procesów decyzyjnych*. WNT, Warszawa 2002.

[15] Stefanowicz B.: *Wybrane zagadnienia infologicznej analizy informacji*. WN Novum, 1999.

[16] Szczepaniak H.: *Inteligentny system zarządzania eUrzędem państwowym za pomocą decyzji dekretacyjnych.* Praca magisterska pod kierunkiem dr inż. Jerzego Tchórzewskiego, Katedra Sztucznej Inteligencji, Instytut Informatyki, Wydział Nauk Ścisłych, UPH, Siedlce 2006.

[17] Tchórzewski J. (2010) *Unmanned System Development Engineering on the Basis of Intelligent State Administration*. Information System in Management V [ed.] Karwowski W., Orłowski A., SGGW. WULS Press, Warsaw.

[18] Tyszka T.: *Psychologiczne pułapki oceniania i podejmowania decyzji*. GWP, Gdańsk 1999.

[19] Wiliński A.: *Kreowanie społeczeństwa informacyjnego poprzez listę Malingową. Oblicza Internetu-architektura komunikacyjna sieci*. Agenor Hoffman-Delbor, 2007.

[20] Zimmer A.: *Identyfikacja obiektów i sygnałów - Teoria i praktyka dla użytkowników MATLABA.* Politechnika Krakowska, Kraków 1998.