MŰEGYETEM 1782

NKTH
National Office for Research and Technology

Péter Pázmány programme

Established by the support of the National Office for Research and Technology.

annual report 2008

BME INNOVATION AND KNOWLEDGE CENTRE OF INFORMATION TECHNOLOGY

CONTENT

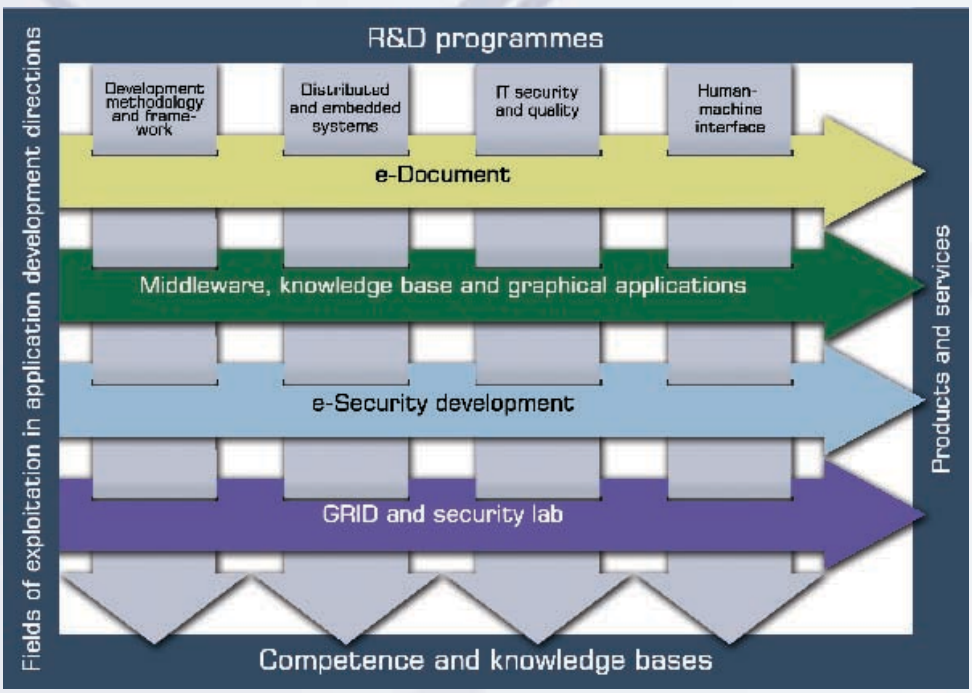
MISSION STATEMENT

Dr. Risztics Péter Károly
associate professor of BME,
director of BME (IT)²

The favourable tradition of the Budapest University of Technology and Economics (BME) and that of its partners has given rise to the strategic goal of the BME Information Technology Innovation and Knowledge Centre at aiming to enhance the competitiveness of the region, and in a wider context, that of the Hungarian economy by stepping up the knowledge content of products and services, creating knowledge-intensive jobs and increasing the number of technology-intensive small and medium sized enterprises in the field of information technology and its applications. A direct means of achieving this strategic goal is exploiting the results of the joint R&D programmes in actual market economy application development projects. The jointly developed, continuous and focused R&D programmes, in addition to reaping new scientific achievements, value-added applications (products and services alike) and major economic developments, also forge and reinforce the frameworks of co-operations in the field of technology transfer-based innovation. They also provide their participants with a source of revenue, thus lay the economic foundations of sustainable long-term financial support.
The results of the Knowledge Centre exert a positive impact on university training and education, as well as on the modernisation of the curriculum. By taking part in the work of the Knowledge Centre, BSc, MSc and PhD students gain first-hand experience and insight into up-to-date and relevant industrial practices.

EXECUTIVE SUMMARY

The co-operation between the university and its industrial partners within the frameworks of the BME Information Technology Innovation and Knowledge Centre, or BME (IT)² for short, had twofold objectives: on the one hand, it aimed at creating research and development intensive, value-added products and services for use with complex IT systems applications as well as producing internationally marketable technology and application development results; on the other hand, it expanded the scope of co-operation between the university and its partners, and formed the basis of long-term self-sustainability by setting up practical innovation automatisms and business models.The results of the R&D programmes are utilised in four major (product and service oriented) fields of exploitation and in the developments they give rise to. To attain the innovation objectives, the rules and procedures were formulated with the requirements of the application development projects borne in mind:



The objectives of the application development portfolio:

1. e-Document
   - Content and document conversions
   - Authenticity and quality control
   - Document management

These projects, linked with the existing products of the industrial partners, aimed at updating existing modules and developing new ones by putting into practice the theoretical achievements of the research. This group of projects fell within the primary field of experimentation and application for the research into development methodology and frameworks, thus, also determining how the development framework was to be enhanced. Moreover, the model-based methodology, framework and technology capable of efficient generation of applications using the set of operations developed for e-Document management are marketable products themselves. Within the framework of the project group, a document conversion service was developed and deployed.

2. Middleware, knowledgebase and graphical application
   - Middleware development framework
   - Transport logistics
   - Geographic information system databases
   - Internal security algorithms
   - Real-time rendering methods

There is an ever-increasing market demand for integration of complex, heterogeneous subsystems into a system with a single system image. Within the project we have analysed the frameworks of the major suppliers and built device-independent code generators to support developments for heterogeneous platforms.

In the field of traffic logistics, the workgroup aimed at elaborating integrated applications for traffic solutions and financial settlement, as well as preparing the deployment the of e-ticketing system. We have developed a middleware application implementing logical functions and services that is suited to the IT systems of the transport service providers. The architectural design, deployment plan and materials supporting the deployment of an e-ticketing system were also elaborated in the course of the project.

Once the knowledge base of algorithms of internal protection was completed, a CD/DVD burner module was also developed to extend the algorithm. This module is charged with managing optical media, specifically to monitor if classified data has been copied to storage media. The module is also capable of tracking optical media. The cornerstone of its operation is the most precise identification of the media possible. To this end, we have come up with a procedure, taking into account various features of the data and the disc itself.

In the field of real-time image processing we have set up parallel simulation-visualisation systems. The rationale behind this was that we realised that not only the visualisation, but also the whole simulation of the process was worth calculating on the graphical hardware, given its significantly greater computing power of than that of the GPU. This entailed the redefinition of the simulation process to match the basic steps with those of image synthesis. The principle, when put into practice, yielded a fluid simulator working with particles and with grids. It also gave rise to a piece of software calculating in real rime how radiation spreads and strays. The fields of application of the programs are engineering design and medical technology, especially radiology and enhancing.

3. PET-SPECT images.
   - e-Security development
   - IT quality laboratory
   - Log-gathering any analysis
   - Virtually closed networks
   - Evaluation of firewalls

Due to the increasingly sophisticated nature of attacks, information security calls for scientifically grounded answers. In the field of e-security development, we have developed procedures and devices that provide protection against the leaking of information from the premises of the institution, which are capable of processing status reports of sizeable networks and making them manageable as well as capable of setting up secure channels of communication (being able to transmit voice) from node to node in an insecure network environment. Besides developing the new procedures, their proven security was also to be ensured. The security lab that was formed is equipped to prepare new products for compliance with Common Criteria methods as well as to analyse and certify the IT security of existing products.

4.0 Grid and IT security laboratory
   - Distributed and extended file systems
   - Industrial application of Grid systems
   - IT security laboratory

The rapid and dynamic development of network technologies enables the creation of geographically distributed, global IT systems pooling massive storage and computing capacities. Owing to the use of Grid technology, these systems make it possible to use algorithms and methods that would have been unimaginable even a few years ago. Example of such tasks include storage and processing of results obtained from the Large Hadron Collider (LHC) at CERN, which resulted in the infrastructure known as EGEE (Enabling Grids for E-sciencE), as well as the domestic ClusterGrid system.

Efficient use and scheduling of resources, as well as security and redundant storage of data are the cornerstones of such systems. In accord with the duties of our partners, the problems dealt with within the projects of Grid and security lab application development group concentrated on the difficulties of synchronisation of vast file systems, on the possibilities of application development for Grid technology, and on application development related to security issues of such systems and applications.

Besides industrial partnerships forged during using Grid technology, we have also formed close cooperation with several international R&D and infrastructure development projects in the field of Grid technology.

The organizational statute provides for the tasks, rights and obligations of the bodies and the operative management. The management co-ordinates the actual implementation of tasks in the project that were laid down in the research, development and innovation work schedule as agreed upon by the Directing Body.

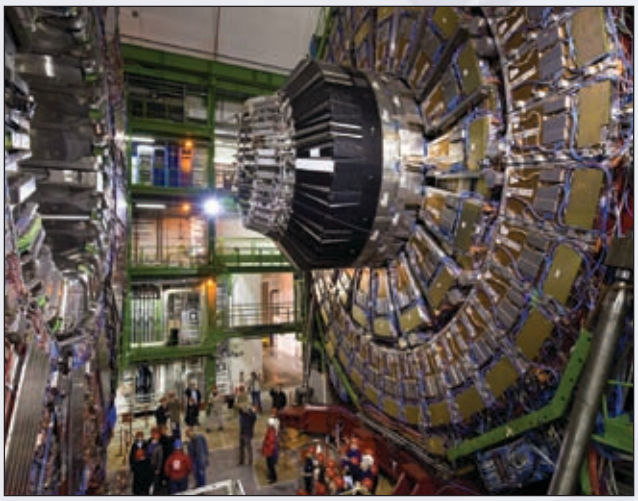
The area of operation of the BME $(IT)^2$ was provided by one of the in-house university partners, the Centre for In-

Major consolidated indicators of accomplishments in BME Information Technology Innovation and Knowledge Centre

1	Exploitable achievments of projects		Consolidated plan	Consolidated fact
	New developments	product	11	12
		service	11	11
		technology	11	13
		application	13	19
		prototype	17	21
	Patent applications	domestic	1	1
		foreign	2	1
	Industrial property, trademark, know-how		4	3
2	Human resources		Consolidated plan	Consolidated fact
	Involved in the project	number of university students	53	82
		number of PhD students	41	40
		number of young researchers	16	38
	Researchers granted scientific degree		3	2
3	Economic use		Consolidated plan	Consolidated fact
	Number of new enterprises founded as result of the project		4	2
4	Scientific results		Consolidated plan	Consolidated fact
	Publications (conferences included)	domestic	39	51
		foreign	26	78
	Dissertations	PhD	5	5
5	Other, special monitoring indicators derived from this project		Consolidated plan	Consolidated fact
	Number of courses enhanced with research results from project		21	26
	Number of students involved		2270	3220
	Number of diploma theses prepared from topics in the project		39	38

formation Technology of the University. The investment in infrastructure, resources, working environment and personnel necessitated by the co-operation between the university and the industry provided favourable conditions for the implementation of the projects.

With the help of process descriptions and procedures, the management regulates in detail the centre's financial and administrative operation, as well as the means of direction and control over the development projects. Financial and administrative responsibilities are assumed by the Secretariat, while the supervision and administration of the internal processes of the projects are seen to by the Project Office. The Knowledge Centre uses an MSZ EN ISO 9001:2001 compliant quality management system, and accordingly, the previously audited system was confirmed in 2008 as well.



For seamless co-operation between the University and its partners, we have created – within the Knowledge Centre Hungary's first joint university-industry IT research, development and innovation workshop, where the researchers and developers of the University work together with experts from small, medium and multinational IT firms, resulting in a team of about 30 to 40 researchers and developers.

The 'R&D&I workshop' of BME (IT)2 is the scene of actual and continuous collaboration, as this is where the industrial partners advise the University on the innovation needs of the market. The University's experts then provide the industrial partners with the latest methodology, model-based development frameworks and software production line. The industry and the university are successful in joining their forces to carry out the actual implementation of the technology and application development, as well as in marketing them.
The products and services our R&D activity has given rise to are presented in detail in a chapter on application development projects of the present report, and a summary is also given in the table of indicators. Nonetheless, we feel compelled to list the results of the three-year project we deem particularly important:

• ParcompMark application – an upgraded version of the benchmarking system; TextureVR – texture based, distributed 3D visualization program; RTPara – iso surface identifying 3D visualisation program; SDSS display – a program

demonstrating the SDSS database in real time; Distributed, particle-based fluid simulation application with hardware support; Distributed fluid simulation application on 3D grid with hardware support; RTPara+, IllustVis, GIVis – Global illumination solution program for volume models.

• Parallel Compositing Library, a product that Hewlett Packard won two awards with at the recent Super Computing 07 exhibition in the USA.

• Application of MVCN protocol and technology with Asterix telephone exchange, providing secure and encrypted telephone communications. Vulnerability assessment and marketing of 'secbox desktop 5'. The series was sold by the hundreds in Japan and the United States. Porting MVCN system for next-generation mobile devices.

• Preparing Zorp firewall for Common Criteria compliance.

A new application (operated as a service on Volánbusz Zrt. website) and a prototype application in the field of meta-layer and knowledge base (Online time-table management and advance booking system and EGOV-GSDI (E-Government GeoSpatial Data Infrastructure) based on ArcGIS Data Interoperability technology).

• Development of numerous applications of internal protection; Mail control plug-in, Webmail control plug-in, CD/DVD burner control plug-in

• Elaboration of a new Ethical hacking methodology using new approach, as well as the launch of a service

• Creation of a HP Scalable File Share (SFS) model laboratory.

• Connecting HP SFS system with the Enabling Grids for EsciencE (EGEE) and ClusterGrid project infrastructures.

• Development of a new synchronisation procedure for HP SFS environment, NFS and Samba file systems.

• Elaboration of an algorithm that is capable of reliably modelling the deformation of trussed bridge-beams as well as the creation of a new Grid service that helps determine the size of such beams.

• Application of SDX digital signature architecture in SOA environment and client-side implementation its control under Windows Workflow Foundation.

• Development of a common client application framework for the client application of the product line "FX". This piece of software supports the processing of medicolegal constats.

• General framework of managing software quality metrics for use with ISO 9126 compliant product certification.

• Creation and application of an aspect-oriented, metamodel-based code generation for complex IT systems applications.

• Extension of the code generator to make it able to create XSD, WSDL and BPEL codes from high-level models so as to enable SOA-based integration of complex, heterogeneous subsystems.

• Development of pilot model application for offline signature verification (Autograph 2.0).

• Development and deployment of document conversion service at the industrial partner.

• Enhancements to the signature recognition system, development of a unique curve matching algorithm.

• Using the results of the R&D programmes, we have upgraded the syllabi of 26 courses with significant student involvement (3220 participants).

• All four research groups have yielded significant publications: number of specialised articles and conference lectures internationally: 78, in Hungary: 51. The Knowledge Centre itself organised 26 conferences and workshops.

• In cooperation with international projects, we organised the most important GRID conference of Europe with the number of participants surpassing 600. The 5-day programme included 275 lectures in 86 sections.

During the first three years, the so-called incubation period, BME (IT)^2 relied primarily on community sources. Its efficiency was demonstrated by laying the foundations and innovation frameworks for a long-term collaboration between the university and the IT sector, by setting the optimal practical means of the cooperation and by preparing joint strategic projects that are the basis of further teamwork.

The Knowledge Centre contributed to the reinforcement of innovation processes within the university and to setting how independent research groups of each department participate in a larger, joint project of the university, as well as to the enhancement of the R&D demand intending to BME. Owing to the potentials of the Knowledge Centre – and in the cooperating university departments (Dept. of Automation and Applied Informatics, Dept. of Control Engineering and Information Technology, Dept. of Photogrammetry and Geoinformatics, Dept. of Mechanics, Materials and Structures, Centre of Information Technology) – BME (IT)^2 fosters the modernization of the higher education, training and the curriculum, the enhancement of the innovation capabilities and readiness both of the professors and the students. The results of the cooperation, contributes to the growth in economic competitiveness of its partners. The professional relationships established within BME (IT)^2, and the results of the Knowledge Centre have made it possible to create and successfully operate with the leadership of BME and the participation of more than 70 IT enterprises the national technology platform of software and services, NESSI Hungary.

DIRECTING BODY OF BME (IT)²

The general management of the Knowledge Centre is performed by the Directing Body. The University and the industrial members of the consortium delegate three members each. The body is chaired by the Rector of the University.

Dr. Gábor Péceli
rector of the Budapest University of Technology and Economics, member of the Hungarian Academy of Sciences, chair of the Directing Body

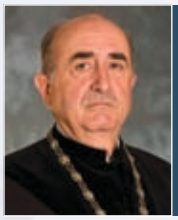
Dr. Ákos Detrekői
professor at the Budapest University of Technology and Economics, member of the Hungarian Academy of Sciences, chair of the National Council for Communications and Information Technology

Imre K. Szabó
general manager of Megatrend Co., member of the Board of the Hungarian Association of IT Companies

Dr. Ákos Reszler
general manager of Nuance-Rcognit Corp., honorary chair of the Board of the Hungarian Association of IT Companies

Dr. Károly Risztics Péter
associate professor at the Budapest University of Technology and Economics, director of BME (IT)²

Zoltán Tankó
electrical engineer, adviser



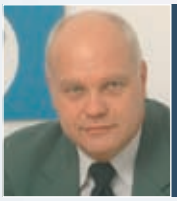
Dr. László Vajta
dean and associate professor at the Budapest University of Technology and Economics

SCIENTIFIC COUNCIL

The Scientific Council reports on the R&D and innovation strategy and projects of the Knowledge Centre, and furthers their implementation. It continuously monitors and evaluates the projects' scientific achievements and publications.

Dr. Péter Arató
chair of the Scientific Council, member of the Hungarian Academy of Sciences, professor at the Budapest University of Technology and Economics

Dr. Gábor Domokos
member of the Hungarian Academy of Sciences, professor and head of department at the Budapest University of Technology and Economics



Attila Haraszti
head of Competence Centre at Hewlett-Packard Hungary Ltd

Dr. Károly Kondorosi
associate professor and deputy head of department at the Budapest University of Technology and Economics, director of science at BME (IT)²

Antal Kuthy
managing director of E-Group Asia

Lajos Lukács
president of DSS Consulting Ltd.

Dr. István Vajk
professor and head of department at the Budapest University of Technology and Economics

János Zelenák
director of development at Navayo Research Ltd.

THE CONSORTIUM

1. Budapest University of Technology and Economics

BME considers its mission to be diversified, multi-level, high-quality education as well as technical research and development. The university ensures that its curricula provide both theoretical and practical training. Accordingly, sound academic foundations are accompanied by practical training with the help of its industrial partners. Besides education, the university lays emphasis on research. As a participant in international research programmes and leader of the national research trends, the activity of BME spans the whole range of basic and applied research, technical product and service development and complex quality assurance.

The high-quality knowledge base present at the university is a firm foundation for the implementation of the R&D projects of (IT)2. Owing to the diverse fields of expertise required by the current R&D projects, (IT)2, the BME Centre for Information Technology, the Department of Automation and Applied Informatics and the Department of Control Engineering and Information Technology at the Faculty of Electrical Engineering and Information Technology and the Department of Mechanics, Materials and Structures at the Faculty of Architecture, are in close communication with one another. Moreover, other departmental research groups that have references and competencies in the fields of expertise crucial to achieving the objectives also take part in the work.

2. Balabit Ltd.

BalaBit IT Security is a developer of special network security solutions satisfying the highest standards. BalaBit is owned by Hungarian individuals. As the only firewall manufacturer in Central Europe, BalaBit has a leading role in the Hungarian market. The company has customers in North America, Australia, and in several European countries. BalaBit IT Security is committed to open standards and is an active member of the open source community. The syslog-ng system logging software, which is the main open-source project of the company, is the world's most widely used alternative syslog solution for the UNIX/Linux platforms.

3. DSS Consulting Ltd.

DSS Consulting Ltd was founded in 1998, its strategic specialty is data mining research and development.

A prominent leveled development workshop has been set up at the company where a tool, algorithm and methodology-irrespective development is being run. There is a close coherence between projects and developments. Theoretical knowledge and research results of the company's experts are applicable for solving problems occurring during practice.

The company has developed and is continuously developing independent intelligent applications on its more significant researches often implemented by involving university partners. This is the way the company's products such as the Bayes Generation bayes network-based data mining tool, the AutoGraph dynamic signature-verification tool, and the WebWatch web-mining system has come into existence. The company has researches on several further fields (i.e. bioinformatics) financed by subsidies obtained from various EU and national tender programs.

4. EGROUP-Services Ltd.

EGROUP researches, designs, develops integrates, launches, represents and operates for its Clients and Partners innovative, IT-based solutions and products generating high business value. Complying with the legal regulations and the international standards EGROUP is a specialist of protected transaction and document management procedures representing high business value, as well as of the supporting IT-transaction, document management and information protection solutions and products. On the Company's cleared-out, triple scale of products, portfolio and technological direction the eDOX™ file and document management system, the Transform™ authentic and safe form and document handling system and the DocMark™ printed document protection system can also be found, among other things.

Pursuant to Act XXXV of 2001 on the Electronic Signature EGROUP developed an innovative document authentication and e-signature technology named Signed Document eXpert, SDX™, being the first in Hungary that was awarded in January 2004 the title „qualified electronic signature application". The success and the value of the solution is indicated by the fact that since that time this technology has been developed into an application platform and it has also become the initiator of several new areas.

5. ESRI Hungary Ltd.

ESRI Hungary Informatics Technical Developer and Commercial Ltd. Was founded in 1989 under the name of GEOCOMP Ltd., and it has been working on this professional area since there are geographic information systems (GIS) in Hungary. Its story is in connection with ESRI (Environmental Systems Research Institute, Inc.) – the leader world wide of the GIS market, American company with 35 years experience - from the beginning.

Our firm is the authorized distributor of ESRI in Hungary. Our target and basic task is distribution and representation of the products and GIS culture of ESRI. Every activity in

connection to GIS and ESRI products – commerce, consultation, support, training, system analysis and planning, system development is included in our profile.

6. Hewlett-Packard Hungary Ltd.

HP is a technology solutions provider to consumers, businesses and institutions globally. The company's offerings span IT infrastructure, global services, business and home computing, imaging and printing. HP holds a number one position in the markets of fault-tolerant servers, UNIX®, Linux and Windows® servers, storage solutions, system management software, imaging and printing devices and PCs, and it is a dominant player of the system integration services market.

The company has operations in more than 178 countries across the word. Since the HP-Compaq merger, it has been serving over 1 billion users on five continents. The development of easy-to-use, innovative products and solutions is fuelled by an annual R&D budget of USD 3.9 bn.

HP leads the Hungarian market of IT services and it has the second largest IT services organization in Europe. In recognition of its efforts, HP Hungary was granted numerous awards including the National Quality Award for business excellence, the Business Ethics Award, the Innovation Award and the Kármán Tódor Award for sponsorship in education.

7. Megatrend Co.

Megatrend Co. specializes in the development and operation of information systems supporting the most important operational, management and security processes of enterprises, public administration and government.

Megatrend provides business solutions in all fields of economy, reached a decisive market share in food industry, by the help of its unique production systems more thousands products are available for customers on the shelves in a day. Its specific integrated administration and production solutions operate in the area of heavy, chemical, pharmaceutical, and light industries. By the help of its Financial and Accounting systems monthly ten billions value of invoices are handled securely. Bank and leasing references prove that the competence of Megatrend's specialists fulfils the requirements of critical business and management processes. The information security product of Megatrend protects business, banking and state secrets.

8. Nuance-Recognita Corp.

Nuance-Recognita Corp. was established in November, 1989 under the name SzKI Recognita Corp. and has been engaged in software development, more specifically, in the design of image processing products, applications, and technologies. Nuance-Recognita Corp. is the subsidiary of Nuance Communications, Inc. (Burlington, MA, USA), the leading provider of speech and imaging solutions for businesses and consumers around the world. Nuance runs operations in many countries, has 53000 employees and its annual turnover reaches 1600 bmillion US dollars per year.

9. Navayo Research Ltd

Navayo Research Ltd was established in 2004 to put a patent, describing a special, virtually closed network protocol in use. Beside developing MVCN network (Manageable Virtual Closed Network) the company is going to be in the market with comprehensive proprietary MVCN solution, server and endpoint products. Navayo presented the MVCN technology at Cebit 2005, the first MVCN network endpoint - a proprietary equipement under codename secbox – and the videophone system development SecVid sponsored by the National Development Agency at Cebit 2006 with great success.

Navayo's mission is to present and propagate the technology, to broaden the productline, to enhance the functionality and usability of secbox, and to develop new MVCN equipments. Hence Secfone do research and development in specified target areas (performance enhancement, mobile communication, video transfer, IP based voice transfer etc.).

10. IQSYS Computing Ltd.

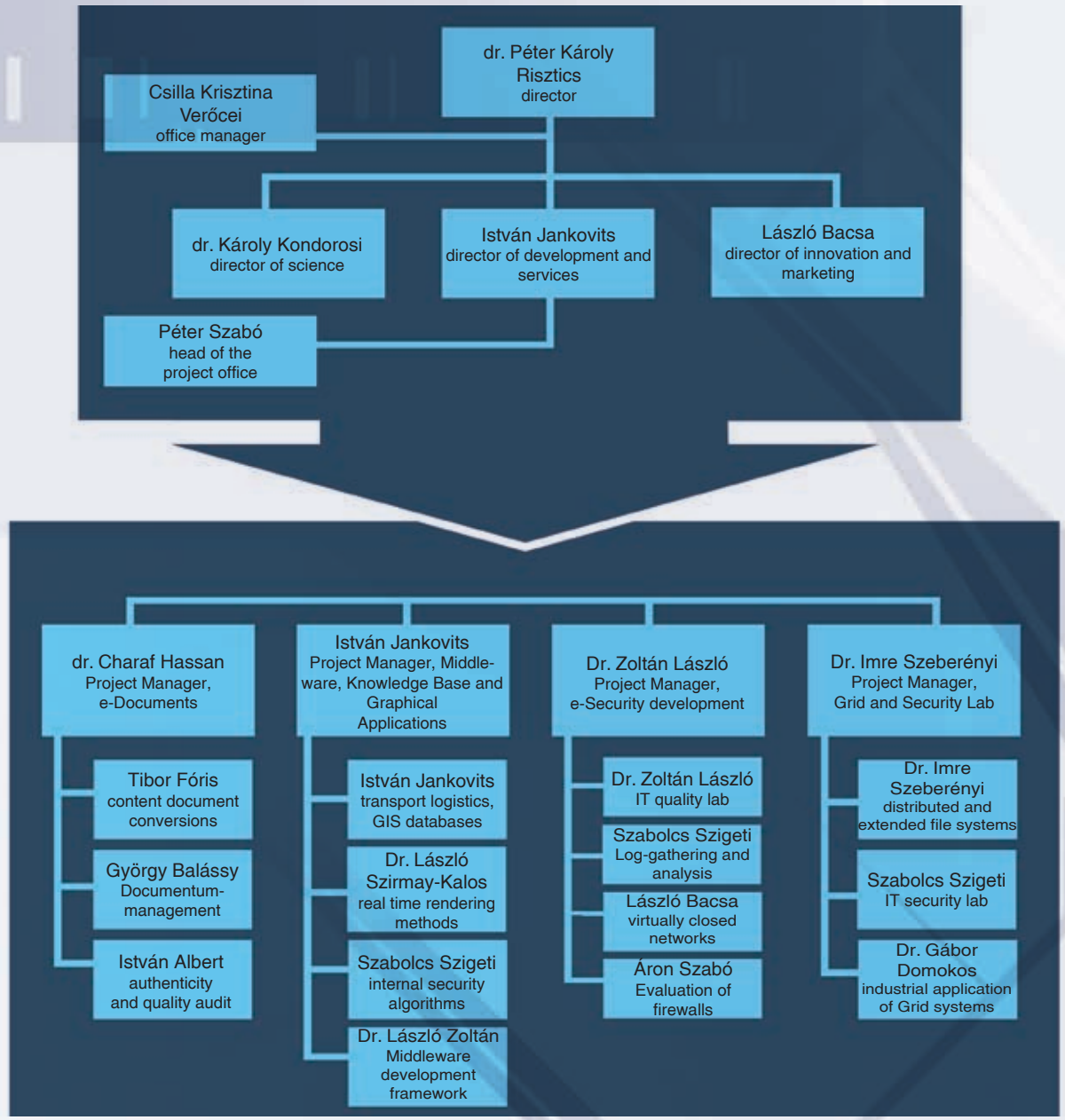
IQSYS Computing Ltd. is one of the largest companies on the Hungarian market specialized at custom application development and application integration. In the way its organization is structured as well as in the everyday practice, our primary aim is to provide high-level services to our customers.

IQSYS offers solutions that suit best to the given task and budget, and conform with the information environment of the company, bringing real profit and value to business. For this purpose, we offer a wide variety of technologies from leading suppliers to free source code organizations. Our consultants understanding the processes of the customers' business, and a team of highly qualified experts are the main contributors to our competitive edge.

We take great care in the introduction and employment of the latest standard technologies which form the basis of the innovative IQSYS solutions. Our strategic partners - BEA, IBM, Microsoft, Oracle and SAS - are leading suppliers on the market, and other technological partners of ours are also prominent in their own field.

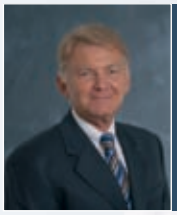
The wide range of solutions applied makes it possible for us to provide suitable solution for each part of business and to successfully resolve complex problems involving several business areas. In the course of its operation, IQSYS cooperates with the other members of the KFKI Group, using the services, expertise and the word-standard products represented by these companies as a supplement to its own competence.

ORGANISATIONAL STRUCTURE



Adamkó Péter • Albert István • Arató Péter dr. • Bacsa László • Bagdány István • Balássy György • Balázs-Piri László dr. • Bársonyné Szegvári Zsuzsanna • Beck György dr. • Béldi Anna Mária • Berényi Zsolt • Bíró Barna • Bíró Imre • Bodó Adél • Bodor András • Bogárdi-Mészöly Ágnes • Bóka Gábor • Bokor Bálint • Borján Gábor • Borsodi Dávid • Budai Józsefné • Budai Péter Richárd • Charaf Hassan dr. • Czifra András dr. • Csapodi Márton dr. • Csapody Dániel • Csébfalvi Balázs dr. • Csutora Mónika • Darázsdi Beáta • Detrekői Ákos dr. • Dévai István • Dóbé Péter • Domokos Gábor dr • Domokos György • Domonkos Balázs • Egri Attila • Ekler Péter • Erdég Szilveszer • Erki Szabolcs • Fábián Ákos • Fábián János • Falus Tamás • Farkas Lóránt • Fekete János • Fekete Róbert • Fodor Péter • Fóris Tibor • Földényi Miklós • Fülöp Balázs • Gábor Ádám • Gál Ernőné • Garami Gábor • Gárgyán Attila • Gavin Brebner dr. • Geda Tamás • Gergely Gábor • Góczán Pálné • Goldschmidt Balázs • Grill balázs Levente • Györkő Zoltán • Haraszti Attila dr. • Harmath Dénes • Hárs János • Hartung István • Hatala Márk • Héder Mihály • Hegedüs Gábor • Hipszki János • Horváth Ádám • Horváth Tamás dr. • Horváth Tamás Imre dr. • Höltzl Péter • Hudák Anikó • Hutóczki Józsefné • Illés Csaba • Illés Dávid • Ilsinkszki Tamás Péter • Imre Gábor • Iváncsy Szabolcs • Jankovits István • Jobbágy Miklós • Juhász Éva • Juhász Gergely • K. Szabó Imre • Kakucska Péter • Kápolnai Richárd • Kardos Gergely • Kelényi Imre • Kereskényi Róbert • Kertész Zsolt • Ketler Tamás • Kishonti István • Kiss Andrea • Kiss Gábor • Kocza Gábor • Koltainé Romvári Ildikó • Kondorosi Károly dr. • Kósa Katalin • Kósa-Pete Mónika • Kovács Dániel • Kovács György Tamás • Kovács Krisztián • Kovács Tibor • Kovács Zsolt János • Kőrösi Ákos • Kővári Bence • Krasznay Csaba • Kuthy Antal • Kuti Gábor • Lakat Máté • László Zoltán dr. • Lendvai Éva • Levendovszky Tihamér dr. • Lukács Lajos • Lupton Glenn dr. • Macskási Réka • Major Csaba • Mári Sándor • Máthé Sándor • Matits Péter • Megyeri Zsuzsanna • Mészáros Krisztián • Mészégető Balázs • Micskó Viktor • Millinghoffer András Dániel • Molnár Károly dr. • Molnár Zoltán • Mónos Tamás • Nagy Ákos • Nagy Ákos Zoltán • Nagy Dezső • Nagy Gyöngyi • Nagy Kázmérné • Nagy Zsombor György • Németh Dénes • Németh J. András • Nitch József • Oszt József • Oszt Józsefné • Pál Tamás • Pálfi Gergő • Pallos Tamás • Pánczél Zoltán • Pasztuhov Dániel • Péceli Gábor dr. • Pelládi Gábor • Péterfi Zoltán • Pilászy György • Plankné Bognár Klára • Pszota Zsolt • Regős Annamária • Reszler Ákos dr. • Risztics Péter Károly dr. • Sás Tibor • Scheidler Balázs • Simon Balázs • Sipos András Árpád • Sipos Róbert • Soóki Péter • Spisak Andor • Suba Gergely • Sulyán Tibor • Szabados Ernő • Szabó András • Szabó Áron • Szabó Krisztina • Szabó Péter • Szalkári Károly • Szántó Boglárka • Szeberényi Ágnes • Szeberényi Imre dr. • Szécsi László • Szigeti Szabolcs • Sziládi Zoltán • Szirmay-Kalos László dr. • Szmrecsányi Márton • Szűcs Gabriella • Tankó Zoltán • Tápai Antal • Tóth Balázs György • Tóth Zoltán • Tóthné Fülöp Terézia • Török János • Újhelyi Zoltán • Umenhoffer Tamás • Vajk István dr. • Varga-Perke Bálint • Várkonyi Péter • Verőcei Csilla Krisztina • Virág András • Völgyi Lajosné • Wagner Endre • Wiandt Bernát • Wippelhauser Tamás • Wolf Zoltán • Zakal Bálint • Zavarkó Gábor • Zelenák János • Zoltáni Csaba

MANAGEMENT



Dr. Péter Károly Risztics

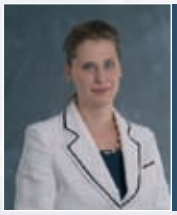
director

Dr. Károly Kondorosi

director of science

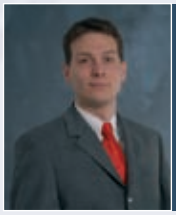
István Jankovits

director of development and services



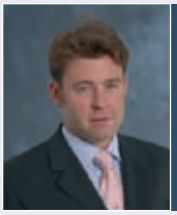
Csilla Krisztina Verőcei

office manager



Péter Szabó

head of the project office



László Bacsa

director of innovation and marketing

QUALITY POLICY

The most important objective of the BME Innovation and Knowledge Centre of Information Technology - BME (IT)² is forging a partnership between academia and industry with outstanding research and development activity and innovation, thus enhancing the R&D programmes of enterprises, bolstering the economic and technical development of the region and consequently improving the economic competitiveness of Hungary.

BME (IT)² fulfils its duties in full conformity with the statutory and contractual obligations, as well as other regulations, and as a result of its conscientious and organised work, meets the demands of its partners to a full extent.

To this end, we use an MSZ EN ISO 9001:2001 compliant quality management system. Quality assurance tasks are dealt with by the quality manager vested with the necessary scope of authority. The management is deeply committed to quality and requires all its colleagues and partners to comply with the quality regulations.
BME (IT)² believes that highly trained researchers with up-to-date knowledge are indispensable to high quality technology and application development. Therefore, the continuous training and self-education of its colleagues are not only required, but also supported. Their progression, mental outfit are follow up.

The cornerstone of our quality management system is the presententation of an optimal outcome. For that reason, we require that our partners and suppliers also comply with quality regulations, and perform their obligations on time. Therefore we constantly monitor our partners and assess them on the basis of how they fulfilled their obligations. In the long run, we intend to co-operate only with those who conform to our quality standards.

For the sake of continuous development, we reveal the discrepancies in our processes and see to their resolution.

We also see to it that our colleagues and partners get to know and understand our quality policy, that they apply it in their everyday work, and that they be aware of their role and importance in achieving the quality objectives.
At the same time, it is our ambition to make our colleagues aspire to quality work.

CERTIFICATE

BP Tanúsító Kft. Certifies that the company

BME Information Technology Innovation and Knowledge Centre

H 1117 Budapest, Magyar tudósok krt. 2.

has established a

quality system
in conformity with

MSZ EN ISO 9001:2001

The Certificate is valid for:

Information technology research & development, innovation

Date of the first Certificate:
2006-07-25

This Certificate is valid until:
2009-07-31

Certificate-Registration-No.:
CERT-25133-2006-QMS

Győr, 2006-07-25

János Papp
Managing Director

THE R&D PROGRAMMES

Computer science and information technology occupy a much less significant position in the economy, society or our everyday life than what would be possible by the scientific and technical level of the field. The two most important reasons hindering a more intensive role:

- The applications are not well adapted to the needs of the users. It is partly because of the lack of established, consensual domain models. Their lack is not well understood, and the problems arising from this fact appear to be flaws in IT systems themselves. On the other hand, these systems are difficult to master, and they are not well accommodated to the workflow and the work environment, thereby placing an unnecessary burden on the user.
- The security and quality of IT systems are not satisfactory. Substantial functionalities may fail and important data may be lost due to system crashes, while security holes make users vulnerable. There is little support to secure operation, and interfaces to other systems are lacking. However, these apparently simple problems can only be solved by complex developments.

For these reasons, BME (IT)^2 was focusing its professional activity on trying to provide users with IT systems that satisfy their needs and that can be used efficiently.

The separate fields of information technology allow independent research to be carried out, and the experience gained can be applied in numerous other domains as well. Development could be carried out under favourable conditions, as the consortium unites experts from a variety of disciplines allowing them not only to carry out intertwined research programmes, but also to nurture a wide range of applications in other domains as well.

According to the work scheme set up in the first year, that is 2006, the work of the Knowledge Centre is categorized into research programmes and application development projects. Research programmes are organised on the basis of professional rationale and provide a steady framework for long term work. Application development projects on the other hand aim at developing specific products or services and, as such, are generally developed in co-operation with our industrial partners. These projects put into practice the achievements of research, while raising new research problems as well. Application development projects are intermittent, and are subject to the time and resource constraints typical of projects. Considering professional and organizational aspects, we have categorized projects into main application development groups. Each group is headed by a project director coordinating the pertinent projects.

The relationships between the research programmes and the main application development groups can be seen in the matrix of the executive summary. This shows that the scientific achievements of the research groups are used in various projects and each project relies on the results of several research programmes. The organisational hierarchy of the Knowledge Centre was formed with the project structure borne in mind, as the projects require firm management due to their money and time constraints. Research programmes are operated by means of another organisational channel (Scientific Council, deputy manager in charge of scientific affairs, heads of programme, Scientific Forum) that mainly uses co-ordinating devices. Accordingly, in this chapter of the report we set out to present the objectives of the research programmes and the most important activities, and finally, we describe how the programmes relate to application development projects. The specific achievements (publications, documents, products and services the projects gave rise to) are described in detail at the presentation of the application development projects.

Main characteristics of research activity during the three years of operation:

- All research groups have yielded significant scientific results, which manifested themselves as publications, theses and know-how. Moreover, they were also put to use in the actual developments and arrangements have been made concerning their future exploitation.
- Several scientific results were obtained by means of a joint work of multiple research groups.
- The problems raised by the industrial members of the consortium generated new research tasks on several occasions.
- Consortium membership for the university partners (departments) has led to increased professional cooperation. The research programmes stimulated, directly and indirectly, university education and helped modernise the curriculum.

Based on the professional community that was established, and on the prospect of ongoing research activities, the Knowledge Centre fully intends to continue its operation.

I. DEVELOPMENT METHODOLOGY AND FRAMEWORK PROGRAMME

Head of programme: Dr. Charaf Hassan, associate professor of BME AAIT

Objective

The following objectives were laid down in the research programme:

Seamless software development technology on an MDA basis

We aimed at developing a model-based methodology that can be flexibly adapted to the various fields of application, one that is capable of handling multiple aspects and is easy to automate. This methodology was to narrow the semantic and technological gap in the existing technology between requirements and models, as well as between models and the code. To this end, a development environment (framework) is created; the application technique of the multiple-layer meta models are enhanced to allow the use of multiple dimensions (more aspects); and the possibility of composing multidimensional meta models is also studied.

The tools supporting the methodology are built into the model handling framework. The results, combined with the results of the component-based development, are also put to use in the area of joint hardware and software development.

Domain specific modelling

The objective was to develop methods that are capable of formally describing the definitions and tasks of the field of application in a way that is intelligible for both the user and the developer, and, at the same time, facilitates the automation of the additional steps of system design.

Information management

We focused on finding a way to efficiently manage and put to use information generated and gathered during development and operation, as well as to ensure adequate data quality and to reveal internal relations present in the data. The results are expected to lead to generalisations and we will be able to apply them upon developing information models, data mining and retrieval techniques of the fields of application,

Handling legacy codes

The new, model-based systems often call for the integration of tried and tested pieces of code that were developed earlier using other methodologies. We have come up with 'reverse engineering' methods that facilitate the model-based handling of legacy source codes.

The actual development programmes were charged with the task of working out a development methodology based on multi-layer and multi-dimensional meta-models – M(LD)M – and a development framework based on this methodology. The proposed framework is of modular structure and can be upgraded with domain-specific modules based on the unified meta-models. This makes application development for the specific domain (in the present instance, e-Document application development group) fast and efficient.

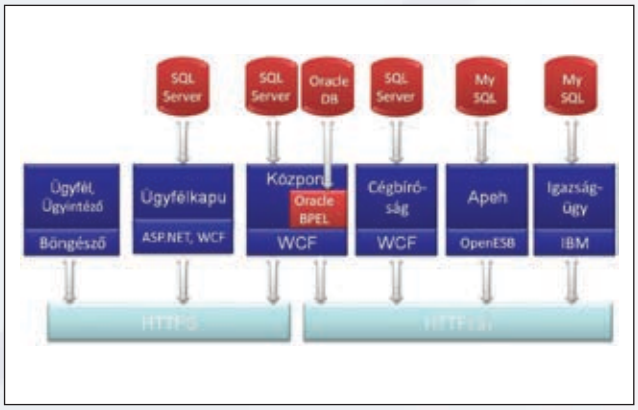
Activities, results

We have taken stock of the achievements of internal university partners of the Knowledge Centre having professional background in the field (AAIT, IIT, IK), and we have settled on the division of labour. After analysing the initial situation, we defined the following main research tasks within the research programme:

- Domain analysis of e-Document, examination of document management by work-flow systems, specification of modules supporting the development of document management software, and design of plug-in extensions to AAIT meta model based frameworks.
- Application of domain analysis and development of domain specific models in the field of geographic information system and traffic logistics.
- Development of source-code models and meta model based transformations to handle legacy source codes, development of compiler-generator technology, and finding refactoring solutions.
- Elaboration of metrics and information management techniques suitable for performance analysis and managing other quality parameters.

The results had a serious influence on various application development projects, from the very first year on. One of the most important influences, for instance, is the advances in methodology as a result of the joint work with our industrial partners on e-Documents. These advances were the reasons Nuance-Recognita was entrusted with major development assignments by its American owner in the so-called Dragon project.

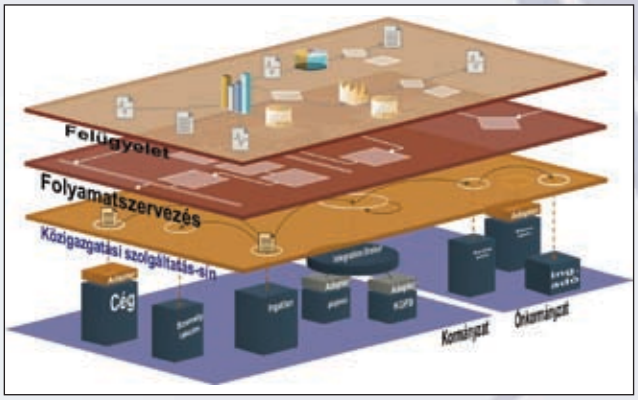
Research into **e-Document** was continued by examining the possibilities of integrating digital signature and workflow oriented document management. Owing to the theoretical result, we have completed the specification and implemen-



tation of the component kit handling digital signature on the client side. In line with the conception of the development framework, we have come up with the workflow and document management support for Windows-based application developments (Windows Workflow Foundation architecture, persistence service). A significant new feature in the development is the definition of the interfaces and functionality of the components implementing high-level work process description, monitoring and supervision. We have also completed the thick client version of the component.

We have developed an aspect-based code generator in the field of research into methods and tools based on source code model for **handling legacy source codes**, and have carried out experiments with positive results to reveal the underlying design aspects of an intuitively designed software system, knowing the UML model and source code of the system. We have also tried to extend the technology to functional languages. We have come up with an Erlang code model, and implemented an Erlang refactoring pilot model, which we tested on real modules with encouraging results. From the second year on, market trends have encouraged us (as a new task, in collaboration with 'Distributed and embedded systems' and 'IT security and quality' programmes) to extend the methodology and the framework to **developing and integrating complex, heterogeneous systems** that are composed of several antonomous or semi-autonomous subsystems and to workflow management.
We studied the methodologies of integration and have come up with a coordination methodology for SOA-based integration. We have determined the main areas of co-ordination, which are the following:
• Acceptance of interoperability standards and requirements: The major subsystems of complex information systems are capable of co-operation by means of appropriate, multi-level (i.e. technical, semantic, organisational) interoperability standards, the maintenance and publication of which require special management methods.
• Acceptance of security standards and requirements: Security requires conscious planning in terms of tools and methods applied on the one hand, and operating environment on the other. Besides selecting and applying the appropriate standards, we also have to set up a system of certifications and qualifications.
• Unification of process description: Operation of complex systems is comprised of regulated business processes. Each process may relate to various institutions or sub-systems. A common descriptive language must be defined to eliminate ambiguities and provide opportunities for consistency checks, recognition of common, recyclable sub-processes. This must be directly executable.
• Acceptance of systems architecture: Defining the architecture of a complex system is one of the prerequisites of interoperability. However, it is of vital importance in terms of maintenance, adaptability and upgradability as well.
• Unification of development methodology and framework: Consolidation and harmonisation of the development methodology and framework with the process description and system architectures ensures a well-organised development, as well as portable and recyclable end results.
• Consolidation of project management: A consolidated project management results in clear-cut and comparable project development, tracking and assessment.
Formation of a joint team of developers:
• As regards process descriptions, architecture and development methodology, we have to ensure a co-operation whose main goal is reaching a professional consensus. A feasible way of achieving this is setting up a team of system developers comprising both independent experts and professionals delegated by the development project in question.

We have set up an experimental system that enables the testing of process description and SOA-based development systems of various suppliers, and examines how they cooperate with each other.
We have extended the application development framework with a code generator that is capable of producing XSD, WSDL and BPEL codes on the basis of high-level, domain specific models. The results of the research programme partly stem from a direct interaction with the 'e-Document' application development project, and were exploited in that field. Other projects whose interaction with the research programme is noteworthy were traffic logistics, GIS and GRID projects. In the project group 'Meta-layer' a new development project was launched in the third year to elaborate a set of tools that supports integration.
The development methodology and framework elaborated within the research programme are intellectual properties with a considerable know-how value.



Plans

Even though the research has already produced an exploitable body of knowledge and a set of tools, it is still open as the domains of application are countless. A possibility of continuing the work is therefore extensive development, elaboration of further domain models.
On the other hand, there are still open questions in the integration methodology. Examples include the methodology of describing workflow processes covering several organisations, process optimisation, consistency checks in case of a large number of processes, optimisation of the architecture implementation by suitable cost functions, etc.
Based on the experience gained thus far, we can state that the methodology and framework programme has yielded the expected results (efficient, logical and manageable development, unified methodology, readable source codes). By extending it and by developing the integration methodology, we can make it possible for a spin-off enterprise launched by the Knowledge Centre, focusing on development and integration, to exploit the know-how developed. This enterprise would possess an up-to-date knowledge that is demanded on the market and therefore, it could have a sound market position.

II. DISTRIBUTED AND EMBEDDED SYSTEMS PROGRAMME

Head of programme: Dr. Béla Fehér, associate professor at BME MIT

Objective

The research programme reported the following situation and set the following objectives:

Distributability and embeddability are indispensable to today's IT systems and they require that certain design criteria be borne in mind. The reasons behind designing distributed IT systems are manifold: on the one hand, it is because of the geographical separation of its constituents, but on the other hand, it can also be due to the design considerations of decomposing the system components. The presence and dynamic development of the Internet has made it clear that extensive distributed systems are only to be designed on the technological basis of the Internet. Furthermore, the design of closed virtual networks of organisations should also be based on this technology. As a result of the advancement of network technologies (bandwidth doubles every 15 months), distributed and parallel systems have become one of the most important means of implementing virtual supercomputers and increasing the performance. In practice, however, distributed systems tend to be implemented as a result of integration, which is often contrary to conscious planning. In the case of integration, individual, and perhaps even heterogeneous systems have to be connected and organised into a single system.

Embeddedness means that IT devices are integrated into our environment, i.e. are "embedded" in our personal belongings. Adapting these devices to the users' needs and creating appliances that can be used without IT skills result in systems that conceal the underlying methods and tools. These novel scopes of application often result in new design priorities, such as minimising energy consumption or providing protection from interference.

The primary fields of research of the group:

Service oriented architecture based implementation of Grid systems

As a result of the improvement of network technologies, researchers have come up with algorithms and methods previously unthought-of, or with those whose implementation was expected to become possible only with the advancement of supercomputers. Grid solutions are a means of integrating network resources and thereby creating immense computing and storage capacities. Our accomplished research objective was working out web service based solutions and developing applications based on these services.

Service oriented architectures (SOA)

Various standards have been created for the interoperability of the components of distributed systems. The most accepted of the latest standards is the Service Oriented Architecture (SOA). Our main ambition was enhancing and doing research into the design and implementation methods of service-oriented components in a way that is compatible with our development framework.

Embedded systems

We aimed at developing design methods that are capable of handling special needs and allowing a joint hardware and software development, which is often required in these cases. These methods were then to be adapted to actual fields of application.

Integration

In this area, we worked out the means of integrating the isolated applications, data sources and data stores into our system. The problem of integration cropped up in different abstraction layers, from among which semantic integration, appearing at higher levels, raised questions. Adequate solutions were then found for them in the research programme.

A number of actual application development projects were based on using the research results of the programme, including 'Embedded and distributed file systems', 'Industrial applications of Grid systems', 'Content, document conversions', 'Document management', 'Traffic logistics', Logging and log analysis', 'Virtually closed networks' and 'Real-time image processing'.

Activities, results

The fields of research developed research tasks specific to them:

- development of parallel algorithms in order to achieve a faster solution to complex problems,
- creating an easy-to-use interface for the distributed infrastructure not only for the programmes, but also for the users,
- load balancing, performance optimisation,

elaborating standards of interoperability and techniques of integration.

Due to the innovation needs of our industrial partners, we have shifted emphasis of the research programme towards distributed systems. Real-life, industrial problems raised various new development needs, whose solutions required research into distributed and parallel systems development (e.g. in the field of image processing or visualisation), and thus postponing hardware-related developments, or, cancelling them altogether, as was case with secbox.

We have developed some efficient parallel algorithms for data mining, analysis of huge amounts of data, as well as tasks of visualisation (in collaboration with the programme "Human-machine interface"). The algorithms were required and used by the projects "Logging and log analysis" and "Real-time image processing". With its several parallel algorithms, its implementation that also uses the GPU, and by exploiting the potentials of the new hardware solutions,

the project 'Real-time image processing' has earned both the Knowledge Centre and its industrial partner (HP) wide international acclaim.
We have developed and improved parallel algorithms that can make use of GRID capacities to solve limit value problems. These algorithms are very useful when solving engineering problems with considerable computing needs, if their solution is possible using common differential equations. Examples of such problems include the calculation of deformations in reinforced concrete structures under heavy load. We developed and, based on the experience, we enhanced the Gradient-adopting Hybrid Algorithm (GHA), an algorithm that helps reduce the exponential calculation need of the former Parallel Hybrid Algorithm to polynomial. This was essential so that our method can be efficiently applied to tasks of greater complexity and more dimensions. The results of the deformation calculation were also tested empirically and they were cross-checked against measured values. We had the opportunity to manufacture and analyse six trussed beams. The disparity between the calculated and the measured results were within 10 per cent, which is acceptable for practical purposes.

In the field of distributed infrastructure design, we concentrated on developing GRID systems. During this process, the activities raising applied research problems and producing generally applicable results were the following: determining factors affecting distributed file system efficiency; development of a scalable file system; file synchronisation based on web services (on SOA architecture); and designing an ergonomic, single system image user interface for the portal. Using these results, we have set up a template system with a web portal interface enabling the users to take advantage of the Scalable File System's 3-terabyte-strong storage capacity and immense computing power. Experimentally, we have connected the template system to the productive GRID system of EGEE (Enabling Grids for E-sciencE), which forms a global resource system of immense capacities, working 24/7. Another noteworthy result of the project is the new file synchronisation method, which is based on persistent messaging. This method is capable of handling distributed file systems of immense magnitudes both with the specialised file system of our industrial partner and with other, generally used file systems.
In the area of integration, the development projects raised actual research tasks. Such tasks included the interconnection of heterogeneous GIS databases used in town management and the compatibility among the IT systems of major transport companies, a problem of the traffic logistics project. Owing to the experience gained in the development projects and to meet actual market demands, research emphasis shifted to SOA-integration from the second year on. In conjunction with 'Development methodology and framework' programme, we have set up a test system for examining the co-operation among the SOA frameworks and developed a set of supporting tools and a development and co-ordination methodology for SOA-based integration.

Our research programme contributed to integration by analysing the interoperability aspect of the professional co-ordination methodology developed for e-Public administration systems. Furthermore, we have developed an implementable method to help determine the interoperability criteria of the 'Traffic logistics' project, and to help up elaborate a data model that is applicable to various transporting companies.

Plans

Based on the results achieved and the needs of our partners, the research programme is worth being continued. However, tasks are to be allocated and organised in the system that was formed during work, that is arranging them according to task types, rather that the system laid down in the objective, which called for grouping in them by fields of speciality.

Parallel algorithms development has bright future prospects both in the field of visualisation and in engineering design. (It is worthy of note that one of the creators of the 'Gömböc', the rightly world-renowned object with one stable and one unstable point of equilibrium, is a project co-ordinator of the project 'Industrial application of Grid systems'; to create the object, they used the method of approximation through algorithms of immense computing requirements.)

In the area of integration, we intend to continue our collaboration with the programme 'Development methodology and framework'.

In our activities up until now, the examination of performance optimisation lacked a scholarly character. It is still justified, however, to study this question in a scientific manner in the future.

III. IT SECURITY AND QUALITY PROGRAMME

Head of programme: Dr. Károly Kondorosi, associate professor at BME IIT

Objective

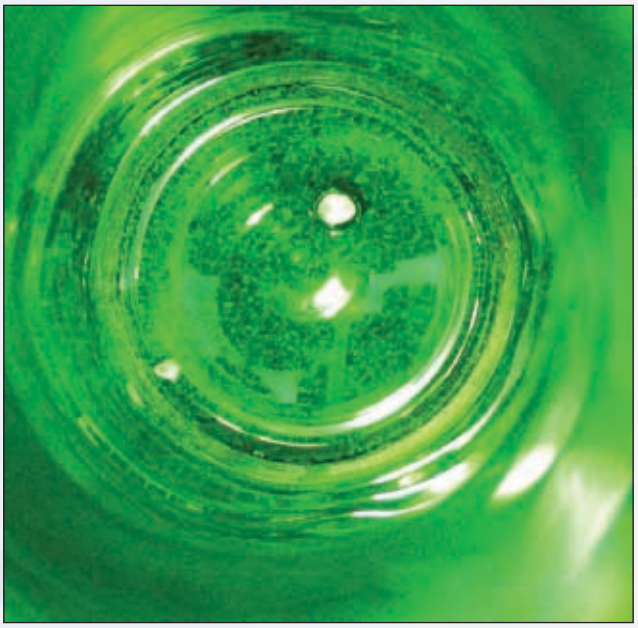
The research programme reported the following situation and set the following objectives:
As IT systems are increasingly becoming part of all walks of life, information security is becoming more and more important. The security of current IT systems is not satisfactory, while security solutions are difficult and over-complicated. To classify the systems and certify their compliance with certain criteria, various international standards have been established (e.g. Common Criteria). These standards are accepted in Hungary, and there is a will to apply them (cf. MIBÉTS). Besides technical approaches, organisational level approaches are also gaining ground (COBIT, ISO27001). Quality and quality assurance are no exception to this, as in addition ISO certifications CMM-rooted certifications are also becoming increasingly popular. The ultimate purpose of the programme for the Knowledge Centre is to create of an IT security and quality assessment laboratory which by the end of the project could become an IT certification laboratory. A university department is ideal for such purposes, owing to its independence of suppliers. Our particular research topics included analysis of new threats, techniques of identification and attestation, secure payment protocols, audit methodologies and their computerised support, as well as determination of quality attributes, metrics and measurement methods of products, resources and processes.

Considering that security and quality requirements arose in almost every project of the Knowledge Centre, and knowing that meeting these requirements is by no means trouble-free, we sought solutions to the actual problems of the projects within the frameworks of the programme as well.

Activities, results

On the basis of ISO 9126 standard, we have developed the quality profile of a piece of software used with measurement techniques. Although product-based software certification has no widely-accepted and established techniques, we regarded the Goal-Question-Metric (GQM) method as normative. We have specified a set of metrics compliant with the standard: external, internal and in-use. On developing the assessment system for the ISO 9126-based certification, we looked into the possibility of finding points of contact with other standards to ease the subsequent deployment. Consequently, we defined the associations between metrics and the phases defined in ISO 12207 standard, which was followed by the specification of relations with further standards (ISO 14598 series, ISO 25000 and ISO 15939).
We have analysed the security and quality certification procedures, and have designed the architecture and system scheme of a generic piece of software supporting these procedures. The system scheme of CMMI Assistant, a piece of software supporting CMMI audit, traces back to this generic scheme and architecture. This software application was used and exploited in the “IT quality laboratory” project.
The Development of information security algorithms project of the e-Security development project group aims at recognising patterns of behaviour characteristic of security attacks. The most important research tasks are the following: building up behaviour profiles on the basis of behavioural patterns experienced during system operation, and developing appropriate methods of risk analysis and assessment. These could help the system reliably recognise potential attacks. The results were summed in a mathematical model that uses several independent factors.

Under the auspices of the project ’IT security lab’, a real-life assessment laboratory came into being, boasting significant success in two different fields:
On the one hand, we have developed the assessment methods and implementation guidelines of evaluating Common Criteria compliance. We have compiled the documentation preparing Navayo secbox for EAL2+-level Security Target (ST) security compliance, according to CC v3.1 standards, as proposed by IABG (Industrieanlagen- Betriebsgesellschaft GmbH). Upon preparing Zorp firewall for EAL4+-level CC-compliant (systematically designed, tried and tested) certification, we had to thoroughly plan every task to be carried out, conduct extensive tests and compile precise documents. First and foremost, a precise and painstaking specification of the tool, product and functions under examination had to be laid down. This by itself proved rather complicated (compilation of Security Target document). Security functions needed examination not only by means of „black box” testing. Software source codes, documentation



specifying design and production and development maintenance procedures also had to be examined, analysed and documented. As a result of our work, we have produced the document package required by the German Bundesamt für Sicherheit in der Informationstechnik office for the certification process.

On the other hand, in the security lab we have specified the principles, methods and techniques of analysing IT systems for vulnerability by means of “secure” external attacks. We have integrated this methodology into ISO27001, COBIT, CC and ITIL compliant examination procedures. Using the results, we offered Ethical hacking services. We have also carried out the vulnerability assessment of ’secbox desktop 5’. After elaborating a detailed professional scenario, we successfully carried out an ethical hacking assignment for a major multinational company in the automotive industry.

We have summarised the preconditions of creating a joint security and quality certification laboratory in a study, pointing out the possible points of contact between security and quality certification. Results of the research and development of various areas, along with experience gained and crystallised in the form of publication seem to confirm that certain connections can be identified between actual assessment systems (e.g. CC and CMMI), and by harmonising the systems, certain pieces of evidence can be mutually recognised.

Plans

Our short-term objective is the exploitation of the results achieved in the field of IT security and quality. The security lab is ready to receive orders for both services (CC compliance preparation and ethical hacking) and is working to develop further IT security services. As regards research into IT quality, our objective is developing a process and product based software assessment procedure for applications of the Open Document Format. Internal, external and in-use metrics are defined in compliance with ISO 9126 principles while performing the task. With internal metrics, we will use the existing results of code analysis. We will create the standards compliant quality assurance scheme by selecting the external metrics that are appropriate for the target field. Using the testing systems and frameworks developed in the project, we intend to examine the ’in-use’ quality attributes of the applications generating Open Document Format.

We intend to continue analysing the relations of security and quality assessment systems and we aim at compiling actual proposals for a means of mutual recognition of evidence to be incorporated into the standards.

IV. HUMAN-MACHINE INTERFACE PROGRAMME

Head of programme: Dr. László Szirmay-Kalos, professor at BME IIT

Objective

The following objectives were set on launching the programme:

This research programme deals with the general questions of interaction between human users and machine systems, manages visual and sonic interfaces and the ergonomics of instantly comprehensible transfer of information. It focuses on, however, real-time three dimensional (3D) imaging. The practical implementation of real-time 3D systems still presents a challenge in terms of computing speed. Realistic imaging and 'telepresence', however, could produce breakthrough results in various fields, such as detecting and manipulating dangerous situations. Another important area is the visualisation of simulations and measurement data (technical design, data acquisition, medical diagnostics), which entails displaying enormous sets of data in a way that is intelligible for the users. This research programme aims at developing new algorithms and methods of realisation.

The results of the research programme were mainly exploited in the project 'Real-time image processing'. The ability to handle large sets of data and the results of algorithm development proved useful for examining samples of signatures within the frameworks of the projects "Authenticity and quality audit" and "Log-gathering and analysis".

Activities, results

Throughout the research, tackling the problems of real-time visualisation of large sets of data was at the centre of attention. In case of measured data, the term 'real-time' is meant to denote interactive alternation of the display parameters and the camera. In case of simulations, it is the processes of simulation and visualisation that run simultaneously, allowing users to control the parameters of the simulated process. In both cases the model can reach the size of several gigabytes or even terabytes, requiring a processing time of nanoseconds per pixels for the experience of a continuously moving object. This task requires scalable distributed hardware infrastructure and parallel algorithms.

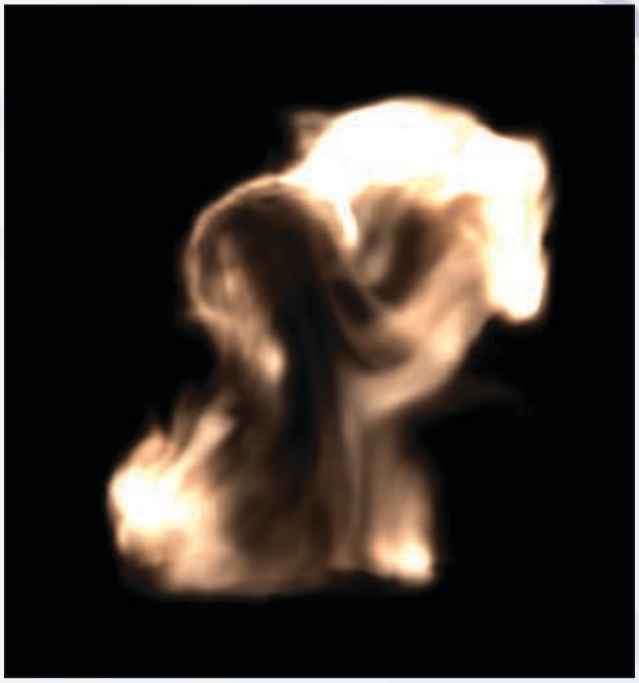
One of the options for distributing the tasks is assigning parts of the model to processors in a way that each processor renders a subset of the visible pixels, calculating how each pixel of that part of the model is affected. In this case, the assembly of the image is done by a final compositing in the image space. Simply by changing the parameters of composition we can influence the visibility of each object and thus we can see behind the objects in the foreground, make them transparent if we wish and we are able to visualise the volume of the objects. For purposes of scalability, compositing must also be done concurrently, in a distributed manner. Our research aimed at examining parallel algorithms of compositing and experimental comparison of implementations.

The more and more widespread use of powerful hardware, especially GPUs raised the possibility of a multi-level application of parallel algorithms, perhaps even in non-business devices. Accordingly, we did research into parallel compositing involving the GPU, and into developing simulation algorithms with general purpose computation on the GPU (GPGPU). The simulation and visualisa-

tion algorithms realised solve problems of hydrodynamics. The third main research group concentrated on new, distributed methods of visualisation. The programmability of the GPUs allows classical location illumination image synthesis to be replaced by solutions offering better (i.e. more realistic and clear-cut) images. Such solutions include use of ambient overlay, ambient lights and illustrative visualisation (emphasis on main parts) instead of X-ray and isosurface analogies.

Research was carried out in close collaboration with our industrial partner (HP's US-based High-performance Computing Division) and the results were incorporated in the enhanced version of the ParaComp compositing library. The product won Hewlett-Packard 2 awards at the Super Computing 07 exhibition in the USA.

Several applications were produced as a result of the algorithm developments. Examples include the scalar field display using distributed X-ray analogy; the ray tracing isosurface displaying application with simultaneous image space and object space distribution, ambient overlay and ambient light; the distributed illustrative display; and the translucent displaying application using the analogy of mistlike light-absorbing materials. Another special application development project was the visualisation of the SDSS (Sloan Digital Sky Survey) astronomic database. The software is capable of estimating distances on the basis of the spectral image of the stars, with astrophysical models that can be alternated even during the process of displaying. The 3D model thus produced can then be explored interactively. On exploring the model, users can validate the astrophysical hypotheses and models and can test what effects they have. Additional applications include fluid simulation and display software with GPU support, distributed particle model and 3D grid model. Finally, a distributed program was developed to determine how radiation spreads in absorbing and straying media.



Plans

Performance data gathered during the project have led us to conclude that parallel systems for visualisation of large sets of data shall be treated as clusters of GPUs, with both simulation and visualisation occurring on GPUs that handle the model subsets. CPU and network intervention is to be kept to a minimum. The applications created are all built on this principle. In the future, we intend to extend measurements to even larger tasks and clusters. To help us achieve our objective, HP donates further units, creating a simulation and visualisation system with unparalleled computing capacities in Hungary (in theory, reaching a capacity of 5 teraflops).

On the other hand, the application calculating and visualising how radiation spreads seems particularly promising. We intend to put it to use to determine the reconstruction matrix of PET and SPECT instruments and, in general, to improve medical imaging methods. This entails the modification of our algorithms that were conceived with the physics of visible light borne in mind to take account of the way higher-energy gamma photons spread (positron emission, relativistic Compton scattering).

APPLICATION-DEVELOPMENT DIRECTIONS
1. e-Document direction

Project Director: Dr. Charaf Hassan, Ph.D., associate professor,
Professional field: Software and systems development
Publications: book chapters: 2, periodical: 25, conference: 130.
Memberships: John von Neumann Computer Society, IEEE, Hungarian Academy of Sciences Information Technology Committee.
Major industrial commissions over the past 3 years: Nokia Research Centre, Microsoft Research, Vultron, ModEduNet EU Project
Professional awards, acknowledgments: János Bolyai research scholarship, 1998-2000; Microsoft development relations regional director, 1998-2006; "For Work at the Student's Scientific Society" Budapest University of Technology and Economics Dean's Commemorative Plaque, 1999; Pannon GSM Professor's scholarship, 2000-2002; Master Teacher's Award, 2001; IT Trainer of the Year, 2003; 2 IBM Faculty Awards, 2004; IBM 48-hour Programming Competition teacher 2004 and 2005.

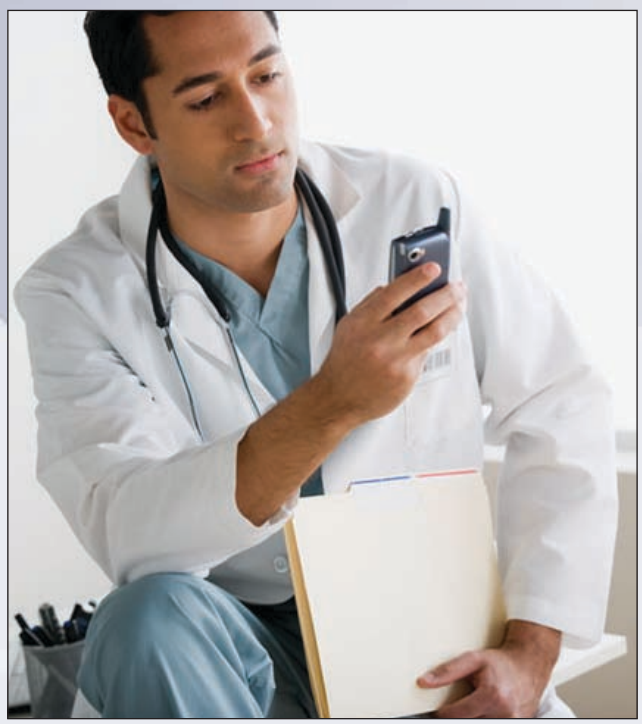
Scientifically grounded methodological research efforts supporting the development of complex information technology systems were articulated as a stand-alone competence in the strategy of the Budapest University of Technology and Economics' (BME) $(IT)^2$ Knowledge Centre. Development work completed in the first year confirms the necessity of methodological research, as well as its important role in the creation of development frameworks that directly support practical applications, because the richness of application projects' content cannot be set in schemes, yet at the same time this cannot be covered with combinations of unique and independent development work in an efficient manner – and it is the time-to-market of products that needs to be kept in mind first and foremost in this respect.

Deployment of the Model Driven Architecture (MDA) software technique constitutes the most modern means of creating framework systems nowadays, and it is a technique that allows visualised transparency and maintenance, and serves application projects by means of ensuring a standard software development technique at the conceptual level. Accordingly, we build around MDA's methodological basis in e-Document application projects, and utilise the theoretic findings accomplished in the field of multi-dimensional, multi-layer modelling.

The framework system provides standard support for shared software development activity in varying application fields from both the methodology, as well as the technology aspects. The objective of formulating different developers' framework systems is to enhance the competitiveness of products containing software development, as well as to create a combination of pooled assets which directly and efficiently activate the code libraries that significantly reduce product times-to-market, along with their elements.

Developer framework system services can be supplemented using application specific plug-in modules. Document management tasks, for example, are implemented with a plug-in module that over and above storing the documents and archiving them directly or as meta data, manages access rights, automatically forwards documents and reply documents to the appropriate recipients, allows for prescribing and tracing the information-flow that documents realise, as well as by means of elaborating the option of mobile document management. Our task is to develop software components that provide services for these products, and moreover to formulate additional editing possibilities for generated electronic documents, along with the possibility to file them in the standard document management chain. With services elaborated for organisation/corporate governance systems, we ensure the possibility to process electronic documents generated during the activation of form completion options in a standard manner, along with the co-ordinated management and system level verification of different documents created as part of the company processes. We formulate an application interface that allows for the articulation of requirements at the user level, and co-ordinates the system of corporate processes and documents accompanying production in a flexible manner which adapts to any possible change.

Within the e-Document Project Group, we use the framework system for development efforts in progress in various professional fields. For users, the convenient and efficient development environment means that they can use high level models, as well as descriptive modes which fit the professional field's concept system during development. Professional, field specific languages have to be formu-



lated for this. Exploring the essential, as well as content related correlations of the applications constitutes the preparations for this phase. This is the work we completed in the first year of the project, among other things, supplemented with performing specific developments which in part accelerate the market entry of planned products and in part ensure that the previously acquired market positions of industry partners can be retained. Wherever possible, we implemented the developments in forms of service in order to be able to recycle the codes.

Development environment and platform play an important role, as regards development. Our project group applies J2EE and .NET technologies for the most part. Considerable expertise in these technologies and the ability to apply them practically are a sound background for further work in the Knowledge Centre.

We have further developed the two projects that we closed in the previous work stage.

Within the project Authenticity and quality control, we made enhancements to the framework and extended it with new mechanisms. Moreover, the project also entailed the development of unique curve tracking and matching algorithms. The three-step model (retrieval of properties, comparison, and classification) has been refined to include five steps. A framework was also developed to enable the independent realisation of these steps. This has a distinct advantage over the previous system. On the one hand, it allows the stand-alone testing of each module and thus the calculation of separate performance indicators on a per-module basis. On the other hand, the development methodology formulated in this fashion is better suited for integration into university education.

Building on the results of the previous work stage, the project entitled 'Document management' has given rise to a framework that could form the basis of future document management projects.

Research and development concentrates on two main fields within the project Content, document conversions, which will keep going in the final phase. The first field aims at finalising the client-side framework, the development of which started in the previous work stage. The other field focuses on developing and implementing a document conversion system at our industrial partner's site.

The university and industry experts collaborating on e-Document project group have complemented the results of BME (IT)^2 with the following:

I. **Content and document conversions (the result is the Dragon MT system):**

• FX client application development framework – basic version, software.
• STAN – client framework, thin version, software.
• OLLIE – client framework, thick version, software.
• MT client – client used by transcriptors, software.
• MTQA client – transcriptor client with quality assurance functions, software.
• Provider client – medical client, software.
• MTSOAdmin client – administration client, pilot software.
• ConversionServer – achitectural design.
• ConversionServer – specification.
• ConversionServer – application.
• ConversionServer – client application.
• Installation of ConversionServer at the industrial partner.

II. Authenticity and quality audit

• A piece of software capable of deciding whether a signature is genuine, photocopied or printed.
• During development, we defined the quality requirements of scanned signature images, and the way they are to be produced.
• With the help of the samples analysed, we have set the parameter value that can optimally distinguish between genuine signatures and counterfeit ones.
• Creation of a modularised development framework with 21 distinct modules.
• Development of a unique curve tracking algorithm.
• Development of a unique curve matching algorithm.

Document management

• Specification, development and documentation of basic, recyclable components relating to digital signatures (electronic signature, timestamp, archiving, authenticity test).
• Specification and implementation of general, workflow-based digital signature system architecture.
• Application of SDX system in SOA environment, implementation of workflow-based control on client side.
• Specification and implementation of a client application providing user interaction with processes, as well as their real-time graphic monitoring.
• Specification and implementation of pilot processes using basic components related to digital signatures, in order to verify the functionality of the architecture.
• Specification and implementation of the shell extension controlling process start-ups.
• Elaboration of a testing plan.

1.1 Content and document conversions (subtask 1.3)

e-Document direction

Project manager: Tibor Fóris
M.Sc. in IT engineering, BME Faculty of Electrical Engineering and Informatics.
Professional field: Software design and development
Publications: journals: 4, conferences: 10.
Professional experience: designing and developing administrative IT systems, developing process control systems, developing enterprise systems and web-based applications.
Major industrial commissions: designing and developing the Standard Administrative System, developing process control systems for Hungarian State Railways, participation in the development of various enterprise, as well as web-based applications.

Our consortium partner, Nuance Dictaphone corporation's, Healthcare Solutions business unit is the world's leading supplier of voice recognition, dictation, and transcription systems (systems capable of creating electronic documents from voice recordings), as well as services related to these topics. Its products simplify the electronic management and processing of patient data, and enhance their quality. Today there are more than 400,000 physicians in about 4,000 hospitals, clinics, and other medical institutions who use Dictaphone solutions containing the Dragon Naturally Speaking voice recognition engine. With its help, the costly activity of writing test findings is replaced by dictation, followed by a quality controlled process of automated voice recognition and transcription with a transcriptor, which makes better and cheaper care possible by means of a more direct, as well as immediate access to electronically stored findings and patient information. According to the development plans of our industrial partner regarding the Dictaphone products, systems that are currently in use will be gradually replaced by systems built on (thick) client-server foundations with a web-based family of products that meet market demands better.

Tibor Sás serves as the subject expert on behalf of our partner. He is a certified electrical engineer with more than 15 years of experience in software design and development topics such as embedded systems, real-time video streaming applications, controlled and configurable automatic document-content conversion, copy protection for software, as well as J2EE and .NET-based business applications.

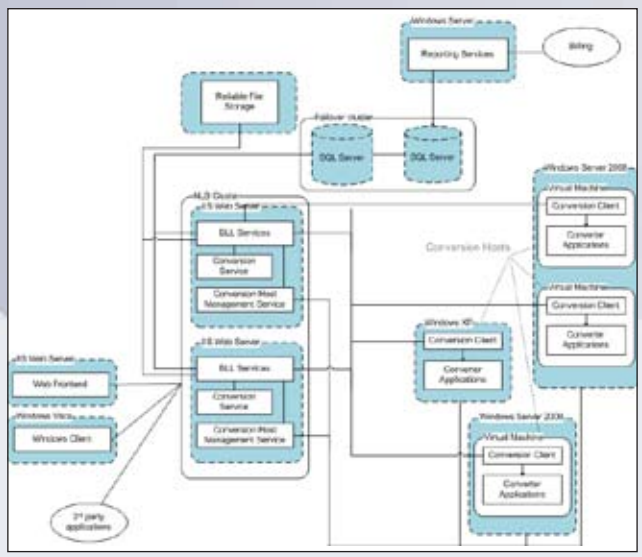
Objectives

In the project, we focus on a special area of document processing, namely on the processing and management of medical reports. Of course, the results of the R&D activities are intended to have broader applicability, to be used as standalone products and/or to be exploited in other document-processing applications.

Cooperation within BME (IT)^2 includes both the development of the Dragon MT Workflow System and the development of the new FX system's clients. For the latter, we are creating a reusable component library and framework system through which document processing client applications can be generated using declarative tools, with formal specifications as the starting point. The most important advantage of the new client system is that it generates customisable applications with standardised operation and appearance, simplifies the integration of differently developed components, ensures the consistency of client-server communication, and provides automatic release tracking. Of course, during the project's design and development phases, server-side tasks must also be solved.

Summary of the activities in previous work stages

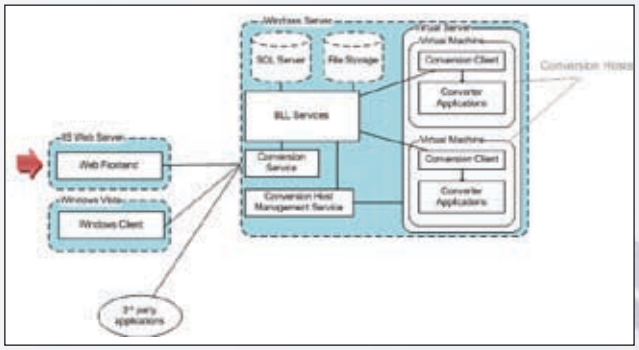
After assessing the existing server- and client-side functionalities, we designed and developed the first prototypes of the FX client framework which will serve as a basis for the next generation client. The development of the framework is iterative, its features and functionality are extended continuously.



In each iteration, new components are developed, and last but not least the continuously changing requirements have to be satisfied. After the development of the basic framework, the foundations of a thin, browser-only version were created (STAN), and a version for developing thick clients (OLLIE) was developed as well.

With the further development of the framework, the so-called server adapter part, which ensures the connection to the heterogeneous server architecture via a common manageable layer was completed as well. During the first stage, in agreement with the industrial partner's product development strategy and scheduling, we participated in the server-side development of one of Nuance's transcription systems. After development and successful testing, the Dragon MT Workflow System rel. 8 went into production.

In the next phase, the first versions of the MTQA client were



finished, which are fully compliant with the UI requirement specification defined by the partner and contains all of the basic operations needed for transcription. These versions also include a series of new features, such as document distribution settings, user profile maintenance, and automatic maintenance of voice data and generated electronic document concordance (so-called Speech Editing). In this phase, a document-model was developed, which ensured handling of the processed content independently from the client platform and the editor.

In subsequent phases of the MTQA client development, we implemented further functionalities such as digital signatures, integration with the dictation software, processing of so-called QA (Quality Assurance) flags required for the quality assurance of documents and transcription work, integration of log functions to measure efficiency, formatting and fact-extraction related functionality. Also during the second work stage, the first two versions of the provider clients were completed. This client software will be used by medical professionals, and will provide them with functions useful in the processing of medical reports. Examples of such functions are dictation creation, content processing and control, document distribution, server-side database access, fact-extraction and categorisation, tracking of document processing, etc.

Summary of the activities in the third work stages

At the beginning of the project's third work stage, the first implementation versions of the framework had been implemented and the applications built on the top of the framework having basic functionality were created.

Developments effectuated in concordance with the industrial partner's needs and plans can be categorized into three groups: consolidation and re-design of the framework, further development of the framework and application development. Applications based on the framework are developed at various locations across the world; the industrial partner built a quite large team consisting of designers, developers and testers (approx. 100 members). Elimination of bugs emerging during the use of the framework, the re-design tasks and framework consolidation was done within the BME $(IT)^2$. Further development of the FX framework was also realised within the project.

Applications developed within the project, the MT, MTQA and the so-called Provider clients were extended with new functionality such as the enhanced versions of workflow operations, processing of patient data, splitting and joining of documents, editing of text and speech concordance editing, to mention only the most important ones. Some of the developments belong to the product family's new functionality, therefore their implementation implied server side development too, in which the BME $(IT)^2$ also participated.

The developed FX framework proved its viability and usability, the applications developed based on it are solid. The use of declarative tools and components allow for efficient creation of consistent applications. Applications have passed the test processes, integration tests and quality assurance processes of the industrial partner, the products reached the ready to manufacturing phase.

Products were also successfully tested in real-life situations in hospitals in the USA.

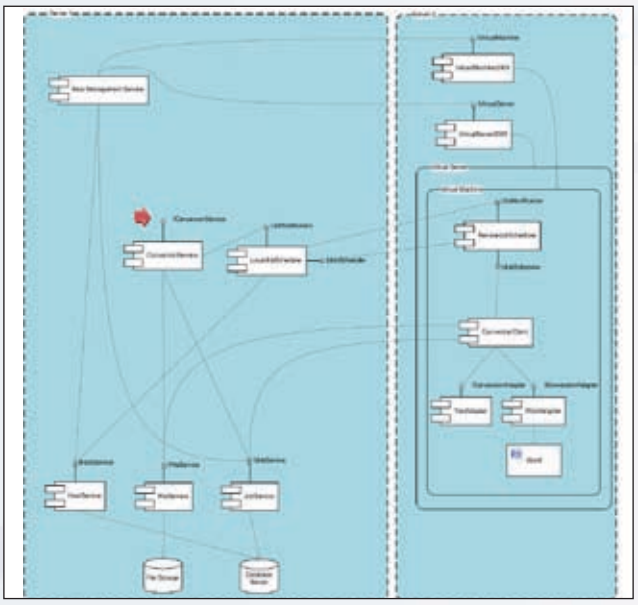
Whether talking about speech recognition or converting PDF files into plain text documents, Nuance has accumulated a wide knowledge regarding document conversion. However, currently this knowledge is scattered among several different modules of independent systems. A new initiative has been started to define and implement a server product which is to serve as an extendible document conversion server, (mainly, but not exclusively) based on the core technologies and competences owned by Nuance, like PDF printing, PDF conversion to different formats, text to speech conversions, etc.. We created and implemented an architecture in which the different conversion applications of Nuance can run in an isolated virtual environment, thereby preventing a scenario where the failure of a single module could lead to the crash of the whole system. Virtualization also enabled us the fast resetting and restarting of converters and a wide horizontal scaling of the system. To synchronize the work of the different converters and to automate the management of the virtual machines, 3 separate management applications were created. External clients can only access the system through these applications, which still allows them to take advantage of the full range of conversion services provided by the system while shielding them from the details of the conversion, like the location or implementation of the actual converter modules.

Several performance tests have been performed on the system. Our results showed significant difference between the performance of the two major virtualization platforms (VMWare and Microsoft Virtual Server 2005). VMWare performed 10-20 percent better in all scenarios therefore we agreed to use it as the primary virtualization platform. Further optimization could be achieved by redirecting the majority of (virtual) disk operations to a RAM disk, thereby accelerating the read and write operations. All these optimizations resulted in a 50% performance increase over our first test results. In the last phase the system was introduced to a broader (but still internal) audience inside Nuance allowing a wider scale of testing. To support this, an AJAX-based web client was created, allowing the users to access the system over the internet from any location, and to test the capabilities of the system.

On the basis of our current results, we can affirm that the system has an outstanding throughput while delivering a stable and reliable service. When the testing phase finishes, further development work can begin which aims at the creation of an out-of-the-box application and a commercial service based on the current conversion server implementation.

The results and products of the project

- Dragon MT workflow system release specifications, document.
- Dragon MT workflow system release 8, server release, software.
- Dragon MT workflow system release 8, thick-client prototype, software.
- Performance analysis, optimisation; study, publications, document.
- Investigating Java and .NET platform integration with the help of web services; study, document
- The design of various client framework system functions, document.
- FX Client functional prototype, software.
- FX client specifications, document.
- FX Client application development framework – basic version, software.
- STAN - framework thin-client version, software.
- OLLIE - framework thick-client version, software.
- MT Client – transcriber's client, software.
- MTQA Client – transcriber client with quality assurance functions, software.
- Provider Client – medical client, software.
- MTSOAdmin Client – administration client, prototype.
- ConversionServer – architecture design.
- ConversionServer – specification.
- ConversionServer – application.
- ConversionServer – client application.
- Publications.



1.2 Document management (subtask 1.2)

e-document direction

Project manager: György Balássy, BME-AAIT (Budapest University of Technology and Economics, Department of Automation and Applied Informatics)
Professional field: software development, .NET Framework and associated technologies, web-based application and portal architectures, document management and groupware systems.
Publications: book chapters: 1, conferences: 4
Teaching activities: participation in the development as well as teaching of courses on Web portal development and Software Development Tools. Professional consultancy in individual laboratory work and thesis planning.
Qualifications and professional acknowledgements: Microsoft Certified Professional (2001), Microsoft Most Valuable Professional (2004), Microsoft Regional Director (2005), Microsoft Certified Technology Specialist (2007), regular speaker invitation to professional events organized by Microsoft Hungary.

Even though the electronic (digital) signature format had previously been treated differently by various systems, the task of standardization seems to have been solved. This has been facilitated by European and Hungarian recommendations concerning electronic signatures and signature formats, as well as the legal background in which our consortium partner, E-Group has played a major role. The SDX (Signed Document eXpert) digital signature architecture, developed by E-Group, is in every aspect a modern product. Extending it in the spirit of Service-Oriented Architectures (SOA), however, has posed several new problems in terms of application development, scalability and product development. During the entire research and development project, interoperability and standardization have been key issues. Consequently, the resulting document management system is flexible enough so that its components can be reused in virtually every possible system that would require electronic signature. In the course of the aforementioned professional activities, a flexible way of managing elementary processes related to digital signatures (signing, authentication, archive time stamping) has been developed for both the server and the client side, which at the same time provides sufficient level of abstraction.

At our industrial partner's side, the project is led by 32-year-old Gábor Garami, E-Group's Chief Information Officer. He has received his Master's degree in information technology from BME Faculty of Electrical Engineering and Informatics, and holds various qualifications in fields related to Microsoft technologies (e.g., MCP, MCSD, MCSA, MSDBA, MCSE). As a professional consultant, he also participates in university education, primarily as an instructor for students doing their individual laboratory work and as a thesis supervisor. His major fields of interest are transaction and document management, and developing and supporting such systems in Microsoft SOA and Microsoft .NET environments. He is a regular contributor to TechNet, Microsoft Hungary's professional journal. He is an initiator and a regular developer of the SDX (Signed Document eXpert) qualified digital signature application and architecture (DSA) product.

Objectives

For institutions aiming to comply with EU requirements, the legal regulations related to digital signatures demand complex document management processes. Implementing information technology processes that realize such document management processes necessitates a robust IT platform with a high degree of availability, as well as simple and efficient service. Furthermore, the platform should exhibit transparent workflows, for the sake of which elementary processes regarding digital signature management should be modeled at a high level of abstraction. The project objective is researching information technologies with the help of which a system that meets the above requirements can be implemented and whose implementation can be verified by means of prototype processes.

Summary of the activities

As the first phase of the project, we established the frames of group work that satisfy the demands of the research and development tasks at hand, and harmonized development methodologies among university and industrial partners. We systematically organized our knowledge of the SDX digital signature architecture and identified fundamental digital signature components. Additionally, we reviewed the regulations and recommendations related to electronically transacted procedures. In particular,
1. we reviewed the guidelines set forth in the Prime Minister's Office Decree No. 2/2002 (IV. 26.) MeHVM, which pertain to the security requirements for services conducted with qualified electronic signatures and to service providers in charge of such;
2. we familiarized ourselves with the archiving processes set forth in the General Rules of Public Administration Authority

Procedure and Services Act (KET) (SDXM, Tax Authority format);
3. we familiarized ourselves with the decree on the general requirements for document management at public organizations;
4. we reviewed the Minister of Finance Decree no. 20/2004 (IV. 21.) PM on electronic invoices;
5. we reviewed the conversion recommendation pertaining to the technical specifications of the metadata of electronic duplicates, as issued by the Ministry of Informatics and Communications.

Next, we performed a requirements analysis of SDX's SOA service and specified the fundamental design principles. We formulated an SDX SOA system specification and designed the system architecture, for which we performed a scalability and performance analysis. The architecture has proved to be fault-tolerant and highly reliable in a virtual environment. We analyzed the developer methodology and group work support system of the Microsoft Solution Framework (MSF), and investigated whether this technique can be used in accordance with the project's requirements.

In the first stage of the second phase we relied on the experiences gained in the first phase as well as the experiences of our industrial partner in working out the requirements which would have to be met by a system managing the digital signature process on the client side. As part of this work, we identified the components which would provide digital signature functionalities when incorporated in a given but otherwise arbitrary process. As the final step of the planning stage, we worked out the simplified prototype processes that have demands similar to those in everyday practice, and which would therefore be useful in the formal verification of the system's functionality.
In the second stage we defined the architecture of the system based on the Windows Workflow Foundation, and implemented the Windows service that runs the system engine. Meanwhile, inter-module communication was specified, and the communication interfaces were implemented. Throughout the development of the system, we kept the intended generality of the architecture in view, which guaranteed that the end product would be a system that could manage larger-scale and more complex processes as compared to the realized prototype workflows. For this end, we implemented a persistency service in the workflow engine, which ensures high reliability and availability. After the implementation of the system engine, we developed workflow components that realize the conventionally recognized elementary steps in digital signature processes. The next step consisted in building a system that automatically generated documentation based on the source code of the workflow activity components thus created. In order to test the reusability of the workflow activity components at the binary level, we engineered several simple processes, which were in turn incorporated in the prototype processes defined in line with the objectives of the project after the finalization of the testing stage. The architecture thus created allows embedding both E-Group's SDX application as well as any other system supporting the SOA architecture. Meanwhile, the system exposes a graphically defined, workflow-based control interface with a high level of abstraction.

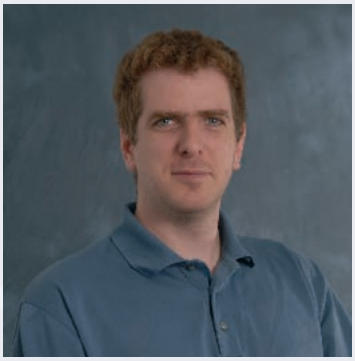
To start the workflows, we created a shell extension closely integrated into the operating system, which makes it possible for the user to start a digital signature-related job without starting a distinctive application, thereby integrating document management tasks into everyday work. To monitor running processes, we developed a thick client application, which shows the real-time status of running processes via communicating with the workflow engine. As part of the monitoring application we developed a custom visualizer component, which can provide a graphical view of the complete process as well as the present state of the workflow. The implementation of functions that provide interaction with the running processes was also carried out as part of the monitoring application.
In the last stage of our work we drew up a testing plan, for which the workflows and the components constituting the workflows were realized in a self-documenting way.
During the course of the project such reusable components and prototypes were created that proved the usability of the applied technology in the domain of document management. Since the components created perform atomic operations in the process of signing documents digitally, the outputs and the experiences from this project are directly reusable in solving any document management problem in a workflow-based approach.

The results and products of the project

- Software development to engineer elementary software components associated with digital signatures (Receipt logging and receiving over different protocols, Electronic signature, Time stamping, Notification, Archiving, Authenticity verification, Delivery, Presentation, Ciphering and encryption)
- Methodology to support the creation of archiving processes that are natural in the frames of KET (public administration authority) procedures
- SDX (Signed Document eXpert) server component, WebService with SOAP (Simple Object Access Protocol) interface
- Data link interface and architecturally scalable SOA system concept specification and implementation
- SDX SOA-based system specification, logical and physical system design specification and implementation
- System pilot for implementing basic functionality
- Electronic invoice format, SDX MELASZ electronic signature format schema and concept repository
- Specification and implementation of a general, workflow-based digital signature system architecture
- Application of the SDX system in SOA environment, implementation of its workflow-based operation on the client side.
- Specification and implementation of a client application providing real-time graphic monitoring of workflows and user interaction with processes
- Specification and implementation of prototype workflows using atomic, digital signature-related components for verifying system functionality
- Specification and implementation of the shell extension controlling process startup
- Test plan

1.3 Authenticity and quality audit (subtask 2.1)

e-document direction



Project manager: István Albert
Certified IT engineer, BME AAIT,

Professional field: Informatics, software architectures, application optimisation

Publications: books: 1, conferences: 5.

Major industrial commissions over the past 3 years: Hungarian Financial Supervisory Authority (PSZÁF), OTP Bank (Hungarian National Bank), T-Systems, Deutsche Telekom

Whether a signature is genuine or not can have a relevant role in numerous contexts. Within the project at hand we have surveyed the possibilities of marketing an application for off-line signature verification and the conditions of developing such an application.

In the course of the project we concentrated on AutoGraph, an application for dynamic signature verification, which was developed by DSS Consulting Ltd prior to this project. The efficiency of this application competed with the best solutions at SVC (Signature Verification Competition) in 2004. The application successfully recognised 100% of forged signatures, and rejected only 4% of signatures that were rejected.

Special time sequence analysis and data mining techniques have enabled us to proceed with dynamic signature verification more effectively than similar solutions have done in the past. Other subproblems of signature verification examined are off-line verification (examining scanned signatures) and originality verification (examining whether a signature has been produced by means of ink or by plotting, photo-copying, etc.). Our R+D activities are aimed at increasing effectiveness in the subproblems mentioned above.

The project leader on behalf of our partner is the company's innovation manager, Andor Spisák. His responsibilities are to supervise and coordinate the activities of the company's R+D team, and to lead funded and other projects within the field of data mining. He has achieved results in the fields of infocommunications and data security. His publications include four papers in conference proceedings, lecture notes for two courses and eight papers in printed or electronic form. He is a member of the John von Neumann Computer Society, and is leading numerous industrial and funded projects. Andor Spisák also participates in writing FP7 proposals for the company. He gives lectures on a regular basis in Hungarian higher education (he has held courses at The Budapest University of Technology and Economics, Gábor Dénes College and Dunaújváros College).

Objectives

The overall objective of the project is to produce a software package tackling today's relevant written signature problems. Typical problems are dynamic and static signature verification and verification of the originality of signatures. Keeping in mind that DSS had already developed an application for dynamic signature verification prior to the project, we only had to develop algorithms for static signature verification and originality verification in the course of the project. Our main objective was to reach the level of effectiveness required by business users for both applications. Consequently, by making use of controlling methodologies, we developed a software product to be marketed based on quality standards.

Summary of the activities

The objective of the first stage of the project was to establish the scientific criteria as well as the technical background for research to examine known signature identification methods, as well as to formulate a proprietary solution. We reviewed previous research findings and set up a development and teamwork environment. We have begun a literature review phase and as part of this we have determined the definitive research policies and elaborated the schedule in light of those. A project portal was created to simplify team- work and co-ordination. We have conducted a counterfeiting experiment in order to measure the level of efficiency with which an average individual can fake as well as identify fake signatures. The collection forms were drafted on the basis of experience from which the database is continuously being expanded. For the pre-processing phase a framework system was created which is capable of processing A4-size scanned forms automatically, can identify the signatures on these, and place them in the database.

Processing is broken down into three major areas:
- the extraction of features
- research and development of comparison algorithms
- research and development of classification algorithms.

In the course of our efforts, we managed to extract features that are valuable from the semantic perspective as well, instead of abstract solutions that tend to stray from graphology characteristics. End-points, crossings, and curves were highlighted. We have formulated an algorithm that is capable of identifying as well as characterising the corresponding features per pairs of two signatures on the basis of the global relations of these features. This allowed the efficient separation of original signatures from counterfeit ones.

At the seconde stage of our research, we identified those significant differences that were relevant when distinguishing between original and forged signatures. Among others, these differences comprise the typical yellow dots that appear on photo-copies and the sharpness of the contours of signatures. In order to make sure that these differences were present in the case of photo-copied signatures we had to choose hardware components of appropriate quality to scan the signatures as well as photo-copy them. It must be noted, however that if hardware components of poor quality are used for forging, forged signatures can be spotted by plain eyesight without the help of any sophisticated application. After the selection of the hardware components we started to collect and scan signatures that would be used to teach the algorithm. In the course of our research we found that seven scanned versions of each signature were necessary. The scannings show relevant parts of the signature, the help of which original and forged signatures can be told apart. These relevant parts are described in more detail in the research report of the project. Furthermore, the levels of the necessary colour thresholds had to be determined. Both the levels and the colour thresholds are presented in the research report. We performed a threshold levelling operation on each scanned image and fed the results into a database. First, we studied the graphs of the different values as a function of the threshold levels. Due to the nature of the problem it did not seem appropriate to apply a linear model for the categorization task, so we chose to use a combination of logistic regression and neural networks instead. While building our model we found that stamped forgeries did not necessarily have to be studied separately, since the properties of such forgeries were included in those of plotted and photo-copied ones. The algorithm developed was implemented using the Matlab software package. The application itself does not contain the implementation of the model, only the separation level that we believed was optimal was included. We chose to use a data mining product to calculate decision vectors that could separate original signatures from forged ones. This was a step demanding particular care since the efficiency of the application strongly depended on the correct choice of such parameters. The product was tested on new signatures different from the ones the model was built on, which helped further refine the model. After finalising the product we obtained an application capable of separating original signatures from forged ones. The threshold levels and the parameters of the decision vector can be manipulated in a separate configuration file. Thus, the sensitivity of the application can be influenced. This is important because each new sample adds to the effectiveness of the application, as the number of samples directly correlates with the accuracy to which the application can be tuned.

Subsequently, we shifted our focus back on processing the graphological features of signatures. The three-step model (retrieval of properties, comparison, and classification) has been refined to include five steps. A framework was also developed to enable the independent realisation of these steps. This has a distinct advantage over the previous system. On the one hand, it allows the stand-alone testing of each module and thus the calculation of separate performance indicators on a per-module basis. On the other hand, the development methodology formulated in this fashion is better suited for integration into university education. Individual students could join the project more quickly, and if they decided to abandon the subject at the end of a semester, their work would still prove useful and complete. Two areas are laid particular stress on during the development: one is retrieving the outline of signatures, and the other is matching the retrieved curves. To streamline the signature a unique curve tracking algorithm was developed, which is adjusted to the features of handwriting. The basic idea of the algorithm is that a small circular section is made from the signature, and the procedure is repeated from the common areas of the circle and the signature curve. The computing needs of this method are negligible, as it does not even necessitates the enumeration of all the pixels, yet, it is able to reproduce the original curves of the original signature highly accurately. Though the system is still being developed, we have presented our partial results at a number of international conferences, where our colleagues showed keen interest and also provided us with valuable advice, which we implemented in our system. As far as we know, this is the most significant research project in the field domestically, with promising partial results and an upward tendency. However, to reach the level of industrial applicability, a further 1 to 2 years of research needs to be carried out.

The results and products of the project

- Creation of the project portal, and developer environment
- Specification of the signature collection methodology, as well as storage
- Collection of signatures, and creation of signature database
- Literature review and formulation of detailed research plan based on consultation with experts and on our own experiments
- Implementation of test system
- Specification and implementation of signature preparation algorithms
- Examination of DPM and HMM-based comparison algorithms.
- Formulation of unique point-pairing algorithm
- Creation of operational test prototype
- Completion of AutoGraph 2.0 application specification and system design

In compliance with our objectives, we developed a product capable of distinguishing original signatures from ones that were forged by means of photo-copying or plotting. Other products that were completed are:

- developer's documentation,
- research report, which comprises the detailed description of methods applied during the development determined during the research phase,
- test records,
- implementation of the learning algorithm,
- database containing scanned signatures used for teaching.

2. MIDDLEWARE, KNOWLEDGE BASE AND GRAPHICAL APPLICATION DIRECTION

Project director: István Jankovits, deputy manager in charge of development and services at BME (IT)², deputy manager in charge of RD at BME Centre for Information Technology, MSc in Electrical Engineering
Field of interest: High level logical synthesis, information systems design, electronic public administration
Publications: 2 books 1 chapter in a book, 3 journals and 22 lectures at conferences.
Major industrial and research projects in the three previous years: Development of the IT strategy of the National Communications Authority; Study on the integration of IT systems at the Communications Authority; Assessment of data assets at the Authority; Introduction of the Unified Financial Administration System at the University of Veszprém; Quality assurance of SzÜR 21 introduction at the Communications Authority; 1st phase of the development of NAVA (national audio-visual archive); Study on the rules of interconnection of integrated databases
Awards: 2nd prize at the National Conference of Scientific Students' Associations (consultant)

The highly specialised and diversified business world (commerce, traffic, public works, public services – including electronic public administration) is facing the challenges of ever-increasing market demands, keener and keener competition, and the requirements of cost efficiency. If economic operators are to meet these challenges, they are compelled to change their attitudes and way of doing business. In today's information society people can rightly expect to receive complex services, which is, in most cases, only feasible as a result of co-operation between various service providers. It is also legitimate to expect that the issues of co-operation and financial settlement between the providers be dealt with by themselves, easing the users of this burden. The convergence of – historically segmented – services and service providers poses new challenges to the IT sector, too. Efforts to integrate services, optimise co-operation between certain fields and business process orchestration are no new to business operators. Adequate supporting IT systems have also been deployed to some extent. As this process unfolds, services will converge and become indistinct and they will no longer be associated with a single service provider.

Complex services require complex IT supporting systems that provide the users with a single access point where they can reach all the services they need without having to bother about unnecessary details (process mapping, financial settlements, clearing amongst multiple service providers, etc.). Although the creation of such services stands to reason, their implementation is by no means self-evident, and demands considerable expertise methodologically and technologically alike, therefore requiring a wide-ranging co-operation and interdisciplinary approach to the issue. To successfully perform this task, we have to see to the creation of an efficient and regulated co-operation between the existing industrial and public administration organisations and systems, and we have to provide the general public with a secure and efficient access to the system. The development plan of Hungary for the period 2007-2013 entitled "New Hungary" specifies the modernisation of public administration and the implementation of electronic public administration as one of its particular operative programmes. This entails the development of a complex service similar to the one we described above and whose implementation is only possible with adequate competences in complex IT systems development. To meet these objectives we have to clearly specify the requirements, standardise the technology and comply with interoperability and security requirements. Cost-effective development of such systems is only possible if the system is defined from a technological, design and organisational point of view at a high level of abstraction, in its own context, using cutting-edge, well-founded methodologies. Upon design we have to take note of the fact that tried-and-tested target applications and sub-systems already operate at traditional levels of operation. The unified service to be developed herein is, therefore, not a completely new investment, but rather the integration of existing sub-systems to form a new system based on their interoperation. For that reason, the methodology we apply has to cover the preconditions of unification and the possibilities of interoperability, bearing in mind the commitments the EU harmonisation entails. Our objective is the deployment of systems capable of adapting to the changing world. However, each and every system component has to be prepared for compliance with interoperability, IT security and quality standards and regulations using the latest technologies (three-layer technology, SOA, ESB, etc). The definition of standards is, obviously, followed by the key objective of creating techniques that allow us to measure compliance or non-compliance with the help of precise metrics. With those techniques at hand we can proceed to certification, which is a significant mission of the BME (IT)² security and quality project group.

The aim of the project group is to participate in various projects in the domain of industrial and public administra-

tion, as well as to synthesise and document the experiences gained throughout the project. We also strive to include the latest results and experiences of the R&D activities in the project and to prepare methodological, standardization and regulation proposals. The Knowledge Centre has two strategic aims: firstly, we intend to pass on and make the best use of the knowledge acquired here, and harness it in the field of electronic public administration. Secondly, we try hard to actively participate in the creation of an electronic service between the public and civic sphere.

Several results of the project group have been put to use in the New Hungary Development Plan projects aiming to modernise public administration. The project group closely co-operates with the GRID, Security laboratory and e-Security project groups and takes advantage of their findings.

Product-oriented results of the project group:

• Middleware development framework

The project entitled Development framework for SOA-based integration was initiated by BME (IT)[2] in the third work stage. The motivation behind initiating the project was the recognition that there is significant market demand (in the banking sector, public administration, healthcare) for integration of heterogeneous systems as components to reach a common end. Experience gained during the implementation of other projects of IT2 has proved that a major part of developments building upon various platforms can be performed in a device independent framework, too. In the course of this project we have developed methods and deviced that enable the creation of a Single System Image of IT systems managed by independent units that are already complex solutions by themselves. A testbed for interoperability analysis of SOA systems was developed and implemented and a device independent code generator was built to support developments for heterogeneous platforms.

• Transport logistics

An evaluation of the basic IT systems and service processes of three major traffic service providers was performed. On the basis of service processes common to all three service providers, the interoperability criteria for their systems was set up, and then we went on to determine the development tasks deemed necessary, and developed the system plans related to the developments. The completed implementation and elaborated the syllabus for deployment and education.
We have developed a new application which uses cutting-edge Web technology to enable users to reserve seats on bus services and provides them with timetable management services. We have elaborated a preliminary study which prepares the process-oriented integration of on-board instruments to the major supporting systems of traffic logistics.
We examined how integrated e-ticketing systems could be introduced, popularized, and incorporated with other payment systems (e-parking, student card, etc.), paying due regard to best practices in the EU and elsewhere in the world, as well as the operating circumstances of the three major traffic service providers.

• Geographic information system databases

A pilot middleware application was developed that helps connect various GIS-applications. Data interoperability can be defined on a graphical user interface. The application supports roughly 20 different, widely used GIS data types, but also enables users to handle completely generic user-defined formats.
We have developed a pilot application supporting the validation and interpretation of GIS data with several automatisms. This application represents the latest technology and facilitates the GIS data exchange amongst co-operating agencies to a great extent. Its graphical interface assists the definition and mapping of semantic and syntactic rules of data interoperability.

• Internal security algorithms

IT support of internal protection is a relatively new scope of application in the banking sector, public administration and enterprises alike. We have developed a unified set of definitions for internal protection systems and analysed the international experience available to us. A testing environment was also created so as to permit the evaluation of both the application developed in the Knowledge Centre and the products of the competitors alike. The development requirements are then determined by the test results and the actual market demands.
We have developed a new application that allows the definition of the sets of rules controlling internal and external electronic mailing within areas of internal protection. The application also sees to the mapping, tracing and enforcement of these rules. The piece of software can be distributed individually, or as an integrated part of the ISeeSec product family.
We have also developed a new module to manage writeable optical media. The system database keeps track on the one hand of the accessible data along with their vulnerability classification, and on the other hand of all the media the system has come into contact with in the course of its operation. Data copying or writing of sensitive data is identified at an early stage (e.g. launching a CD/DVD burning software), allowing crutial alerts to be initialised and making it possible that a record is kept of the media and affected data.

• Research of real-time rendering methods

In the first phase of the project we designed a customisable benchmarking system for the image compositing device 'ParaComp' of our industrial partner HP. This benchmarking system was then used to study the efficiency of the API and certain applications. We have implemented distributed volume-visualisation applications using various approaches and their examination has given rise to suggestions on how ParaComp API could be enhanced.
We have developed four new applications for the visualisation of large sets of data; we took part in the enhancement work of ParaComp compositor; we have developed algorithms for visualisation tasks with significantly higher efficiency. Research into using the GPU capacity for visualisation, compositing and general-purpose computation on the GPU is also key areas of R&D.

Formerly developed applications have been continuously extended with new algorithms. Besides, real time distributed applications have been implemented in new fields of applications, such as film production or radio therapy. The applications implemented are based on a number of new methods and/or original algorithmic approaches.
The project group contributed to the achievements of the Knowledge Centre with 29 international and 9 Hungarian publications.

2.1 Geographic information system databases /subtask 2.1/

Middleware, Knowledgebase an Graphical application direction

Project manager: István Jankovits

Our consortium partner, ESRI Hungary Ltd., is a Hungarian-American owned joint venture. It was formed in 1989 (with the name of Geocomp) and its main aim is the Hungarian distribution of the products and culture of ESRI (Environmental Systems Research Institute), the leading GIS software maker. ESRI Hungary Ltd. offers comprehensive services in the field of geographical information systems (GIS), willing to complete projects of systems integration, as well as unconventional tasks. It is a large company specialised in the development and integration of GIS-based IT systems. The company profile covers all activities related to GIS (and the ESRI products), including commerce, software support, training and education (general and special), system analysis, systems development, database compilation (together with map and data sheet production), and database integration. Research and Development, such as data interoperability research, are therefore one of the basic activities of the company. The objective of ESRI Hungary Ltd. is to establish world-class GIS software systems and control models in Hungary that could render its users activities more efficient, organised and easy in the field of environmental protection, technical sciences, healthcare, land exploitation, marketing, investment, risk and financial analysis.

The project directors on behalf of our partner are András J. Németh and Krisztina Szabó, graduates of the Faculty of Civil Engineering at the Budapest University of Technology and Economics. After graduating from the university, they successfully completed a Business Management and an MBA course. They boast considerable leadership and project management experience. András J. Németh has dealt with GIS systems development and deployment for more than 15 years now. He has more than 30 publications in English and Hungarian alike in journals and at conferences. He is member of the board of trustees of OpenGIS Foundation and of the organising committee of the Hungarian GIS Conference. Krisztina Szabó has been dealing with GIS systems design and deployment especially in the state sector for 7 years now. She has lectured at numerous GIS and state sector conferences, and co-authored a GIS textbook and several studies.

Objectives

On developing electronic public administration services, we are increasingly faced with the demand to integrate heterogeneous systems that process data files of different types. This integration would lead to the interoperability of information and data stored in these heterogeneous systems. ESRI has encountered and successfully solved such problems before, having had to connect GIS databases with other applications or databases thereof so as to establish interoperability. As the methods and techniques applied have been greatly similar to one another, we have set ourselves the aim of developing a general solution with the help of which quality and quantity examination of external databases can be easily seen to in a process oriented manner. The ultimate benefit of such a solution would be the resulting interoperability of data required by the users.

It requires substantial work to 'admit' databases and data types issued by various data providers, or in other words, to incorporate such external data into the system. Upon incorporation, the system has to check the data for quality and quantity, manage mapping and conversions to ensure interoperability, while assuring data integrity. The effects of the expected conversions must also be traced throughout the process.

In the course of the project we have come up with a solution that enables regulated verification and validation of the data comprising the users' GIS systems.

On developing the pilot software, we applied the widespread SSADM standard. Project management implements a PRINCE project co-ordination methodology adaptation. The adaptation is also justified by the pilot nature, limited budget and the R&D nature of the project.

Summary of the activities

The most significant user group of mapping data is comprised of municipal councils and their associates. The subject of our examination was therefore the location data used in municipal councils.

To begin our work on IT systems integration, we first had to assess, map and evaluate their data structure and functionality. Then, we developed a technical terminology dictionary covering the most essential terms of the field.

We set up a test environment with a graphical user interface to model these IT systems, the topological mapping of their structure of data and function, as well as the possibility of entering or connecting arbitrary data to any graphically

placed object. This was the phase in which the data format was picked, provided the format in question was known.

Transferring data from one system to another might require data conversion. For that reason, we have developed a module with a pilot-level set of functionalities enabling simple visualisation of database tables, entities, fields and other elements, as well as the topological structure of the database by graphically showing the connection amongst these elements. The module also provides quality and content check of the data.

After evaluating municipal IT supporting systems, we have found that the support of primary municipal tasks was handled by sporadic solutions, forming an inhomogeneous cluster technologically and architecturally alike.

The complexity of applications supporting a certain technical field of the municipal council, as well as the uniformity of the supporting IT processes all hinge upon the size of the council, its economic and financial conditions, management principles and plans.

As a result of EU subsidies, the municipal councils have begun integrating the sporadic solutions and establishing comprehensive, unified e-Public administration systems. These systems, however, are typically limited to the internal mechanisms of local public administration with only few services offered to the general public and governmental clients.

Successfully implemented and deployed systems represent the local nodes of e-Public administration processes. To establish electronic government, we must find a way to connect these nodes.

Well-defined channels of communication must be in place to provide for the regulated flow of information. This project aims at proposing and creating “data information highways” connecting the electronic government nodes.

Municipal supporting systems provide for the reception, processing and transmission of data both for their own use and for external organisations. We inspected one of the most significant elements of this process, namely the flow of spatial information. We traced how the data is changed during continuous exploitation from the moment it was created to application in public administration and re-entry into the main source of information due to obligation to supply information to the state. We have also considered the possibilities of secondary exploitation of the municipal data assets.

We have examined and explored all the GIS (map, information system) data, mapping representation data (DAT, special public works maps) and related data (mapping object descriptive data) that the municipal councils possess. We have processed and categorised the data (resulting from official procedures) according to levels of confidentiality.

As a result of the assessment of data flow and exploitation at the municipal council, we have charted the process model of data flow between the external data provider and the municipal council. Upon charting the model, we considered how the means, possibilities and dependencies of supplying data are regulated by law.

We have defined the events of the data verification and acceptance process required to incorporate municipal data, and we have identified the belonging data. We have associated decision cases with events, defined actors, together with their tasks, roles and permissions.

Within the frameworks of pilot development we designed and optimized the supporting process verifying and accepting data. Then we went on to plan the IT system supporting data communication and administration. Development was conducted interactively, touching upon design, development and testing phases alike, resulting in the pilot application of the supporting process.

To summarise the results and lessons of the project we could state that by examining the behaviour and interoperability conditions of spatial data in the municipal system, we have managed to draft and model the municipal spatial data infrastructure of the e-Government system. We have also come up with a proposal for fostering data communications amongst the nodes and data acceptance into the system.

The results and products of the project

- Deed of Foundation
- A dictionary of technical terms
- Pilot project test environment
- Project specification, containing project objective, scope of activities, and professional overview of the project.
- System plan: Application plan of the process verifying and accepting data exchange between the external data provider and the municipal council.
- Testing plan: Operations assessment by means of test cases.
- EGOV-GSDI (E-Government Geo-Spatial Data Infrastructure) tool. Pilot application: Representation of a supporting process verifying and accepting data. This standard-based module is easy to integrate into existing systems, open, inexpensive, easy to customise. It can be deployed and used on its own, that is to say, if certain conditions are met, this module can be made into an independently marketable product.
- User guide: Manual detailing the use of the pilot application.

2.2 Transport logistics (subtask 2.2)

Middleware, Knowledgebase an Graphical application direction

Project manager: István Jankovits

IQSYS Computing Ltd, an affiliate of Magyar Telekom Plc's Business Services Business Unit, started its operation on 1 January, 2008. The enterprise, formed as the legal successor of Integris Rendszerház, IQSYS Ltd and T-Systems Hungary, offers one of the widest range of products, technologies and services on the Hungarian IT market, and at the same time, it is one of the largest companies on the Hungarian market specialised in systems integration and in developing and implementing IT solutions.
Owing to the diverse relations of Magyar Telekom and the international operations of IQSYS and T-Systems Hungary, the company boasts an extensive international background. As a result, its clients are mainly comprised of large enterprises and institutions of Hungary. However, the portfolio of IQSYS also includes solutions and services that address the needs of small and medium enterprises and local governments. With its innovative operation, IQSYS has always contributed extensively to the deployment and popularisation of novel technologies, products and development methods in Hungary. The company is carrying out innovation at present, focusing on solutions that could considerably enhance the efficiency of IT developments and control.

Project management tasks on behalf of T-Systems Hungary Ltd are handled by Tamás Wippelhauser, MSc in Electrical Engineering, graduate of the Budapest University of Technology and Economics. He extended his knowledge in Sybase, SAP BW and Uniface developer's courses. He has several years' experience in the management of software design and development projects. Currently, he is the head of the software development division of T-Systems. His field of speciality is the development and deployment of traffic and traffic logistics supporting systems. References: Since 1996, he has been working on the TransIT project of BKV, where, in addition to project management, he was also in charge of scoping, quality assurance and development. Besides, he also co-ordinated the Volánbusz VBIIR project aiming at developing a traffic-specific system with the name 'TRAFFIC'.

Objectives

Throughout the three work stages, the project aimed at connecting the IT systems of the three transport companies to a pre-defined extent. To accomplish the shared tasks, we had to develop meta-layer logics and service set that function according to the agreement that the companies entered into and provides a standardised interface of communications for each company.

In the course of the third work stage a paper was compiled that projects the future plans of all three transport service providers and assists them in harmonising their future policies.

Summary of the activities in previous work stages

The objective of the first work stage was to connect the IT systems of the three companies. To accomplish the shared tasks, we had to develop meta-layer logics and service set that function according to the agreement that the companies entered into and provides a standardised interface of communications for each company. To meet this objective, the Knowledge Centre, using its research and development experience, held consultation in the design and implementation work stage, while later on, synthesising and analysing the results of the implementation, came up with new, cutting-edge patterns, proposals and standards.

The objective of the second work stage was to develop a domestic ticket sales system capable of integrated timetable management and traveller seat reservation. The researchers of the Knowledge Centre gained considerable experience in analysing interoperability criteria of sizeable IT systems, as well as in creating the interoperability conditions of such systems. The Knowledge Centre has vast references in this field in public administration (the former Ministry of Information Technology, National Communica-

tions Authority, Ministry of the Interior), thus, besides the technology expertise (EA, ESB, SOA, etc.), the workers of the KC are also knowledgeable in relevant standards, rules and regulations. To confirm the results, the Knowledge Centre, in association with its industrial partner, launched an actual R&D project at Volánbusz Zrt.

Summary of the activities in the third work stages

The third work stage aimed at examining how an e-ticketing system could be deployed, a short or mid-term strategy for all the companies involved. The work stage was divided into four phases. The first phase consisted of reviewing EU requirements and directives as well as studying real-life systems around the world. On studying practical implementations of such systems internationally, a particular emphasis was laid on the fact that e-ticketing should be implemented in way that it integrates with other traffic logistic services and subsystems. The second phase saw the elaboration of the e-ticketing system's functional specifications, taking into account the conditions and existing systems at the three transport service providers. On the basis of the needs of the transport service providers, we resolved to reach three main objectives:

1. Improve revenue indicators.

2. Improve operating efficiency.

3. Provide customers with better service.

The third phase aimed at examining how the e-ticketing system could be integrated into the existing corporate environment, reconciling traffic, economic, management and policy aspects. We have outlined the main task groups necessitated by the deployment of the system. In the fourth phase, we examined how the e-ticketing system could be enhanced and extended. By the extension of the system we aim to ensure that the new ticketing system could form the basis of further developments in two directions:

• In public transport: the final objective is the creation of a country-wide interoperable system that allows passengers to use public transport with a single card. This would first be introduced in Budapest and its environs by integrating the systems of Volánbusz and MÁV, thus enabling an interoperable use of the means of transport provided by the Budapest Transport Association (BKSz).

• In non-public transport applications: the goal is to combine the card with other applications, such as (but not limited to) e-parking and student card.

The tasks carried out in all three work stages projected a harmonious co-operation among the three transport service providers. The future plans indicate a willingness to implement the systems, the objective of which is to assist the modernisation of public transport services in Budapest and its environs, serving as a model for other transport service providers in Hungary.

The results and products of the project

• In the field of IT systems interoperability of the transport service providers:
• Description of the criteria
• Changes to data models
• Description of new and modified functions
• Implementation of FORTE-Integrity (database, software)
• Functional and integration test documentation
• User's manual
• In the field of developing an advance booking system with integrated timetable management capabilities for transport service providers:
• System plan and data model for ticket office application
• System plan and data model for Internet application
• Training plan
• Deployment plan
• Development of the testing environment
• User guide and training programme – for ticket office and Internet applications
• Successful key user training
• Functional testing on client-side
• Completion of integration testing
• Documentation of development
• Successful end-user training
• Development of real-life environment
• Real-life deployment of bus and coach station ticket office backup system functionality
• Real-life deployment of Internet coach service vending system
• In the field of evaluating the scope of applicability of e-ticketing systems:
• Description of the criteria
• Design of system architecture
• Training plan
• Deployment plan
• Extension plan

2.3 Internal security algorithms (subtask 2.2)

Middleware, Knowledgebase an Graphical application direction

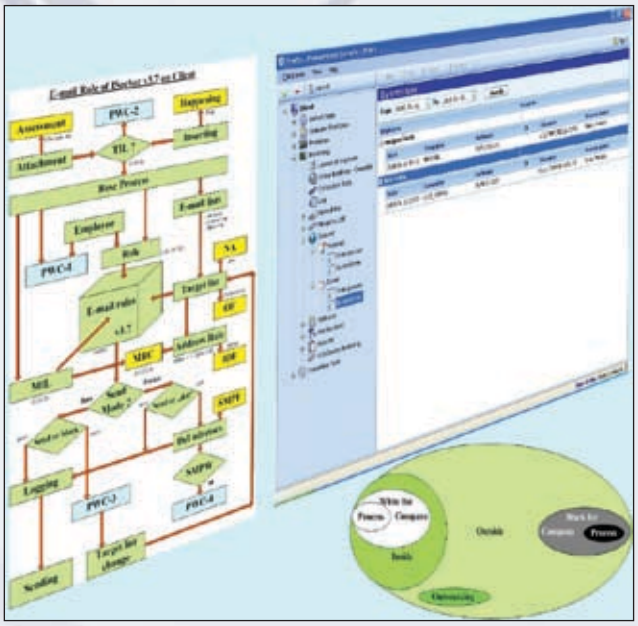
Project manager: Szabolcs Szigeti MSc in Electrical Engineering , MBA, BME IK
Place of work: BME Centre of Information Technology
Specialty: Information technology, computer networks, IT security, next generation internet protocols.
Professional certifications: CISA, CISM, CISSP
Teaching roles: programming, software engineering, computer networks
Publications: book chapters– 3, conferences -17, others 11

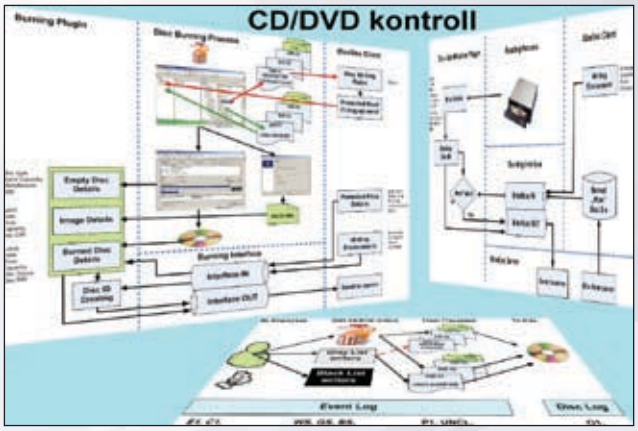
Our consortium partner, Megatrend it ltd., aims to improve its ISeeSec software product. ISeeSec is a complex it safeguard solution, dedicated to the prevention of internal information leaking. Its effectiveness is based on the control of access rights, software applications, output channels and file operations. The product has been awarded with the Innovation Price of the Ministry of Informatics and Communiction, the IT-business Leadeship Award and the European Excellence Award at Cebit. Within the collaboration, Megatrend ltd. Carries out software engineering tasks with the support of experts from BME $(IT)^2$ knowledge centre. Tasks related to the development of the theoretical background are carried out with the active support of the industrial partner. Additionally, the test environment was established and installed with the help of the partner.

Dezső Nagy is the leading expert on behalf of our partner. Dezső Nagy received his M.Sc. Degree in electrical engineering at the faculty of Data and telecommunication of BME. Currently, he works as a security consultant. Among other qualifications, he has a higher degree in security management, as well as BS 7799 security auditor qualifications. He is graduating this year at BME as an IT Security Expert. In addition to fulfilling his working roles in education, development and management, he is the security consultant of Megatrend ltd. His area of specialty is internal threat assessment, focusing on human resources as the main source of vulnerability, as well as the development of the protection philosophy of ISeeSec, and the definition and realisation of its development standards. During the last three years, his research are was the threat analysis of employees and the identification of the security events generated during work. Transposing information events into security events can mitigate risks for information assets. In the next three years, he will be researching the application of data and text mining techniques in finding patters in security incidents. He is a member of the „Hétpecsét" Information Security Association.

Objectives

The project is aimed at creating a tool that is able to detect accidental or deliberate information leaking using behavioural patters. ISeesec has been on the market for 6 years, however, changes in customer demands require that the product be improved. Due to the appearance of new threats and market competition, ISeesec has to be further developed in order to accommodate for novel features. The objective of the project is to develop an improved version of the ISeesec framework. Using newly developed external modules it will be able to identify and prevent generalised attacks, and thus this framework will provide complex services for customers.

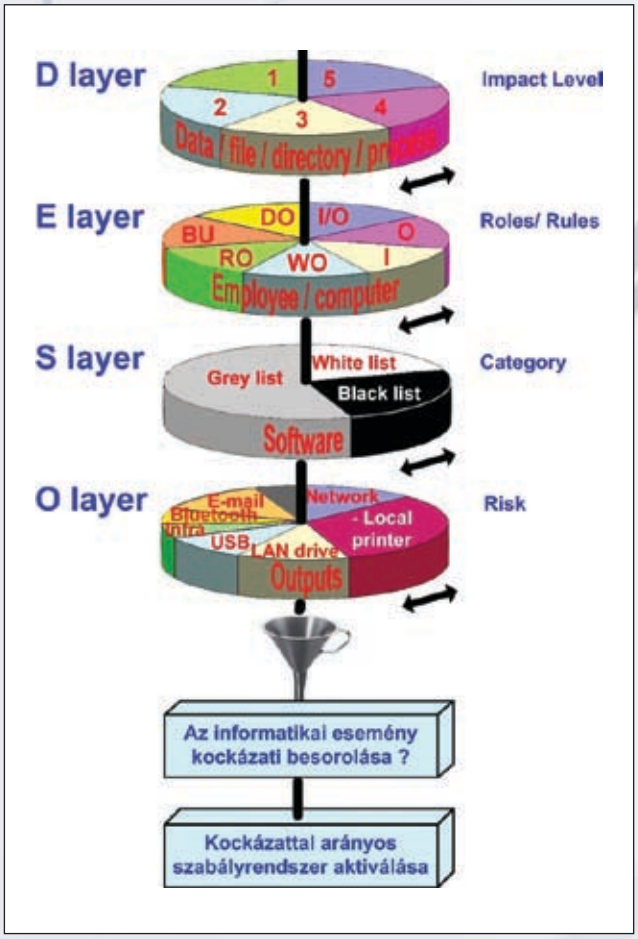




Summary of the activities in previous work stages

The main objective of the first stage was planning. An Iseesec installation was set up in the test bed laboratory at $(IT)^2$ in order to perform trials and comparisons with other similar products. We have also performed a market analysis which includes: analysis of competitor products and the specification of new features, discovery of the need for an integrated it security protection tool for the collection and analysis of security events.

ISeeSec and competing products were compared to find possibilities for improvement. Based on these analyses, planning of new modules started in the second stage. The two planned modules were the email control module and the CD/DVD control module. The mail control module was implemented as an Outlook plugin. A great part of the development was experimenting with the proper solution. The result was a plugin, which may also be used as a stand-alone product for controlling mail.



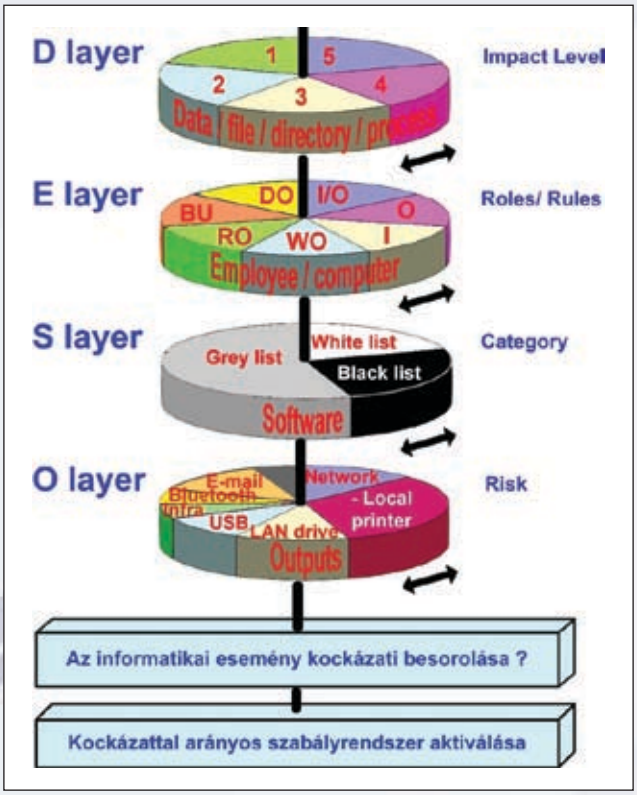
Summary of the activities in the third work stages

In the third stage the CD/DVD control module was implemented. This module is able to control the use of recordable optical media. Its task is to determine if classified information is written onto optical media and to track these disks. These functions are based on the identification of the disks, for which we have designed a method.

Based on the information gathered by the module, a database is constructed, by which the disks and users can be tracked. The module also supervises the CD burning application (initially Nero)to determine the list of files being written to the disk. This enables ISeeSec to stop and audit writing classified data.

During the period the functional requirements for the module were determined, the module was designed, implemented, tested and finally integrated into the ISeeSec framework.

Also, based on design of the email control plugin, a webmail control was developed at the industry partner. This enables the ISeeSec framework to monitor and control information transmitted via web based email.



The results and products of the project

- Market analysis (study).
- ISeeSec improvement plan (documentation).
- Email control module design (documentation).
- Email control module (software).
- CD/DVD control module design (documentation).
- CD/DVD control module (software).

2.4 Research of real-time rendering methods (subtask 1.4)

Middleware, Knowledgebase an Graphical application direction

Project manager: Dr. László Szirmay-Kalos László,
Doctor of the Academy, Professor, Ph.D., M.Sc. in electrical engineering, BME IIT Head of Department
Speciality: Computer graphics
Publications: 18 books, 14 book chapters, 38 journal papers, 79 conference papers.
Membership: „John von Neumann Computing Society" computer graphics group presidency member: 1999- Eurographics executive committee member: 2001- 2004
Notable industry assignments in the last 3 years: Intel Co., Graphisoft Ltd., Institute of Radiology, GameTools FP6 project
Awards: Bólyai scholarship, Széchenyi scholarship, Charles Simonyi award, Bólyai award

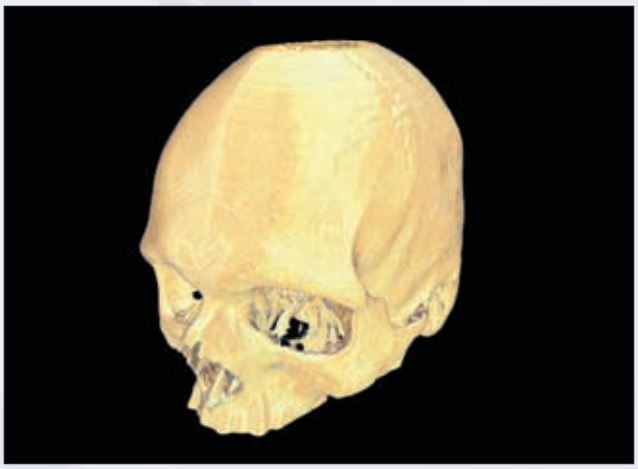
Our partner within the $(IT)^2$ project is the High-Performance Computing division at Hewlett Packard (HP), which designs and develops cluster hardware and software technology supporting integrated computation, storage, and visualisation. In a distributed implementation of a visualisation method, the participating computing resources complete the sub-task assigned to them according to the chosen strategy and their results (partial images) must be combined in order to produce the final image. Combining partial images is called image compositing, which is one of our project's main focuses. Since currently there is no standard software solution for image compositing, HP, integrating existing efforts, developed a specification and an implementation for image compositing, the ParaComp API.

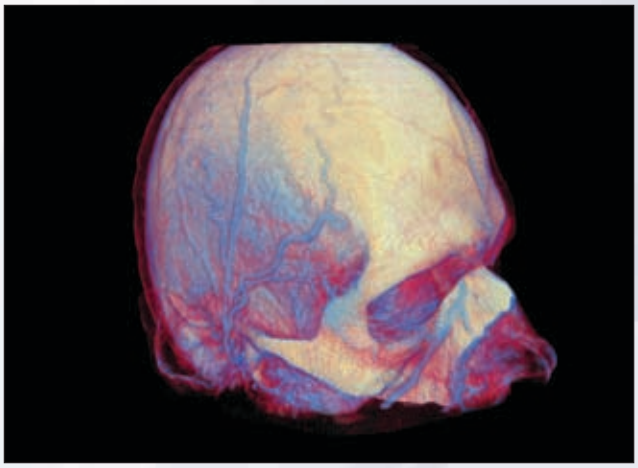
The visualisation methods and applications developed within the knowledge centre are part of HP's demonstration materials for the SVA (Scalable Visualisation Array) and ParaComp products. Developments of the compositing library will be integrated into the product. HP set as an objective for this year that their SVA system should become suitable for general purpose (non-graphical) computing as well, i.e. the graphical processing units (GPU) in a cluster accomplish general purpose computations (GPGPU approach).

Glenn Lupton is the subject expert on behalf of our partner, the technical director for High-Performance Computing Visualization R&D group at Hewlett Packard. He has over 30 years' experience with R&D projects including graphics clusters, image compositing, programming environments, compilers, and software tools, and has held senior technical positions with Digital, Compaq and HP. Since 2007, he has been dedicating half of his working time to coordinating HP's GPGPU development efforts.

Objectives

The primary goal of the R&D activity is the research of algorithms and rendering methods for visualising large (giga or even terabyte-sized) datasets in real-time and the development of applications based on these results. In order to accomplish these goals, at the BME $(IT)^2$, we develop solutions that incorporate new algorithmic approaches which have better algorithmic complexity properties than the existing solutions. On the other hand, we also design and implement parallel and distributed versions with superior performance and/or more efficient use of hardware and software resources.
In the project we work on HP SVA tools. One of our main targets is the investigation and development of the ParaComp compositing library. Besides this, we develop distributed scientific visualisation applications that are based on this compositing system. Concerning visualisation approaches, we focus mainly on volume visualisation methods, and develop solutions and applications for visualising such volume data sets. Data sets from various scientific and application areas (medical, simulations, astrological, etc.) and different visualisation purposes require differ-





ent processing and visualisation approaches as well. In agreement with our partner, we choose for our investigations special areas where the size of the datasets justifies distributed processing and we develop solutions for these application areas. Another important area of our activity is the research of methods for using the graphics processing unit (GPU) for visualisation, compositing, and general purpose computation (GPGPU).

Summary of the activities in previous work stages

In the first period of the project, we developed a configurable benchmark system (ParCompMark) for the analysis of the ParaComp compositing library's performance. The tool allows the study of the ParaComp library under various usage scenarios and the analysis of the scalability and performance increase of applications implemented atop of ParaComp. Algorithms and application prototypes can be easily plugged into the benchmark system, so the performance gain achieved can be measured, the application's performance can be tuned, the tool proved to be useful during the developments.

In the field of distributed rendering, our group released several stand-alone applications implementing some of our research results. We have completed a distributed, ray-casting based volume visualizer (RtPara), which implements both object-space and screen-space parallelization. A translucency based rendering method was also implemented, and we identified some ParaComp limitations and set-up the main development objectives.
Another distributed volume-rendering application (TextureVR) has been developed which uses the 3D texturing functions of the shared graphics cards as a re-sampling tool.

For displaying one of the large-scale data sets, the SDSS (Sloan Digital Sky Survey) project, our group developed a new application. With the optimal utilisation of the cluster's shared graphics hardware, image sequences can be rendered from the database's astrophysical data at interactive speed.

The ParaComp API basically included two kinds of compositing modes: depth-based and alpha channel-based operators, both capable of handling 8-bit data. However, some visualisation methods and applications may need further data formats, operators and functions which are not implemented. We participated in the design of software-architecture changes and implemented new data formats. Development and implementation of other, new operators was also in progress.

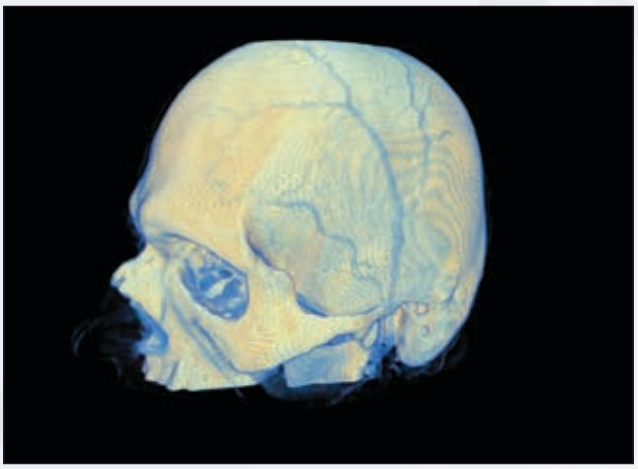
In the second phase, we put more stress on general (not computer graphics related) GPU computations – in the first phase research into fluid movement and dynamics was conducted. Simulations for engineering design and various natural phenomena (flow simulation, cloud, smoke movement, and explosion simulation) are generally based on solving the Navier-Stokes differential equations. The group implemented a distributed, particle-based fluid simulation application and a distributed regular grid based application too. In both applications compositing of the partial results is based on the ParaComp library.

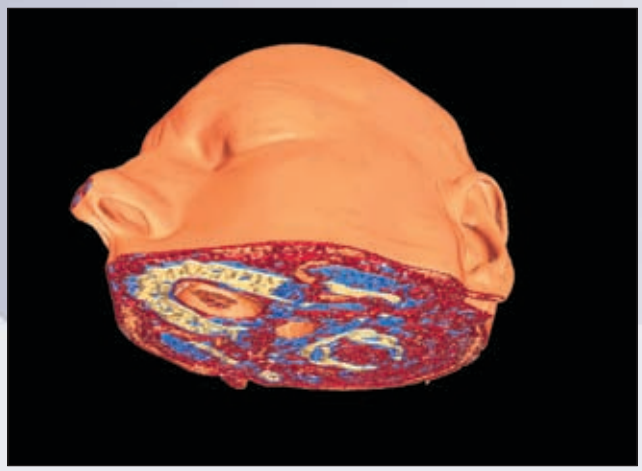
Summary of the activities in the third work stages

Goals of the project's third phase were the finalisation of the floating point and additive compositing functionality of the ParaComp library and mainly the development of distributed GPGPU methods and techniques. The advance of the GPGPU technologies allows the realisation of demanding distributed real-time volume visualisation applications and also the GPU realisation of new simulation methods. Within the first category, we developed a distributed application implementing ambient occlusion shading and environment map lighting, and an illustrative visualisation application which uses style transfer functions. Within the second category, we realised an application solving the global illumination problem for volume rendering which can be used for medical applications (radiotherapy, PET reconstruction).

According to the plans, as regards ParaComp API development, we finished the implementation, testing and documentation of the additive compositing extension, so these features became integral part of the ParaComp core.
On the other hand, distributed visualisation applications were developed for the ParaComp API.

The first distributed visualisation application applies the ambient occlusion shading and environment map lighting techniques (popular in photorealistic rendering and filmmaking), in the field of engineering and scientific visuali-

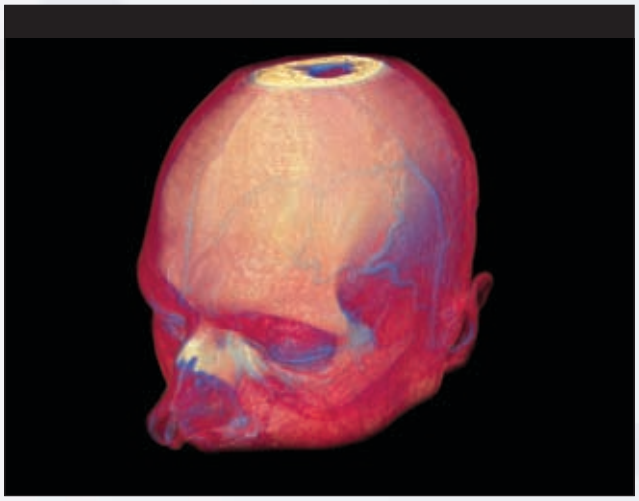




sation. This application is an extension of the previously developed iso-surface rendering application (RtPara). During the shading of the iso-surface, an environment map is used as a light source, and also the method takes into account the neighbouring iso-surfaces' effect on the ambient light. Moreover, the above is achieved without reconstructing the whole isosurface from the volume data. The method, compared to the Phong-Blinn shading, significantly increased the quality of engineering/scientific/medical visualisation without considerable performance decrease.

The other distributed visualisation program is based on the recently appeared illustrative visualisation principles. This means that during the image synthesis, not the optical analogy is used, but the capacity of a human illustrator of grasping the essence is simulated. One approach is the application of a scalar value to visual style mapping instead of the scalar value to colour mapping. The other solution is the automatic increase of the transparency of surfaces having small curvature in the viewing direction. Using these techniques, important details can be highlighted; disturbing effects can be suppressed, so the visualised data becomes clear. This is analogous with the case when a drawing emphasizing the essence is easier to read than a photo containing everything. With the programming of the GPU shaders, we were able to develop a real-time rendering system even with this non-conventional rendering technique.

The GPGPU approach, or simulation-rendering, became more and more important during the project. In these applications both the simulation of a physical system and it's time dependent rendering is done by the graphics hardware. Since the recently appeared CUDA is meant for such purposes, we upgraded our cluster with new graphics cards so that it is now capable of running CUDA programs too.



In this phase, based on our earlier fluid simulation experiences, the goal was the solving of the global illumination problem for volume rendering. Such a method has many possible application areas. One of the examples is radiotherapy, where the position of the internal or external source of radiation must be determined so that cancerous cells will receive the necessary dose while healthy tissues should receive a minimum dose. To solve this problem, photons emitted from the source must be traced inside the body through multiple scattering steps till absorption. Time needed for such simulations is in the order of hours, days even on super-computers. For an efficient mathematical approximation method and the iterative refinement of the initial approximation, we developed an algorithm which converges quickly and can be efficiently implemented on the parallel architecture of the GPU cluster. With this method the placement of the radiation source can be done at interactive rates.

Results and products of the project

- Specification of benchmark system (study).
- Specification of a distributed ray-casting based volume renderer, study, document
- Specification of a distributed translucent volume renderer, study, document
- Prototype of a distributed ray-casting volume renderer, software
- Prototype of a distributed translucent volume renderer, software
- Stereo volume renderer based on ray-casting, software
- ParCompMark benchmark system application, software.
- ParaComp API extensions – floating point pixel format support and implementation of the ADD compositing operator
- TextureVR – texture-based distributed 3D visualization application
- RTPara – isosurface reconstruction based 3D visualization application, which implements object-space and screen-space distribution
- SDSS visualiser – application visualising the SDSS database in real-time
- Distributed particle-based fluid simulation application - with GPU acceleration
- Distributed fluid simulation application on a 3D – with GPU acceleration
- RTPara+ – extension of isosurface reconstruction based 3D visualization application with ambient occlusion shading and environment map lighting, which allow photorealistic visualisation.
- IllustVis – distributed illustrative visualisation program.
- GIVis – Global illumination solving program for volumen rendering.
- Publications.

2.5 Middleware development framework

Middleware, Knowledgebase an Graphical application direction

Project manager: Dr. Zoltán László

This project was initiated by BME Centre of Information Technology. The motivation behind initiating such a project was the recognition that there is an increasing market demand for integration of complex, heterogeneous subsystems into a system with a single system image. The implementation of the e-public administration system entailed development projects with actual application development and integration needs. Likewise, electronic health care systems are expected to give rise to similar tasks, too. A development methodology and development tools need to be elaborated to facilitate the solution of problems that arise. Research results of two Knowledge Centre programmes, namely Development methodology and framework, along with Distributed and embedded systems laid the foundations of the development of such a set of tools. Moreover, BME's involvement in the actual implementation of e-public administration systems provided a potential field of application for them.

Objectives

The research and development aims at developing methods and devices that enable the creation of a system with a Single System Image composed of IT subsystems that are already complex solutions by themselves and are managed by independent or partly independent organisational units. Unsurprisingly, one of the key expectations about the system, besides minimising manual workload of development, is support for fulfilling functional requirements by using adequately high-level models. This also has favourable effects on the flexibility, maintenance properties and variability of the system. Moreover, facilitating the fulfilment of non-functional requirements is also a key factor, particularly for features such as differentiated security and reliability that can be adapted to risks and needs. The methodology must pay heed to the relations within the organisation of development and operating, the autonomy of the subsystems, and the potential of gradable development.

Summary of the activities

The project was completed in the third work stage.
Under the given circumstances and at today's level of technology, both relevant literature and our research consider SOA-based integration to be the best suited for implementation of integrated services comprised of complex, heterogeneous subsystems. Main arguments for SOA: loose interface, clean, modular structure, comprehensive standardisation (on open standards), an extensive range of ready-made software packages.

Actions performed in the course of the project:
1. We have studied, tested in practice and compared the SOA frameworks of several major suppliers.
2. We have elaborated the methods for examining the co-operation among the systems and developed the testbed for performing the assessments.
3. We have evaluated the standards compliance of the systems and revealed the deficiencies of the implementations. We have come to the conclusion that systems are interoperable in terms of basic, service call interface, but there is no other compatible interface of co-operation. The products of each step of development cannot, therefore, be handed over to another system. Another general problem we discovered was the lack of persistence of data exchanged during co-operation.
4. We have come up with a solution to the problem of persistence by connecting the services and message handling systems.
5. We have elaborated how the specification of functional requirements using standardised (UML), high-level models is possible, and come up with a solution for code generation with multiple-stage model transformations.
6. We have developed code generators for the systems of the major suppliers.
7. We have studied the enterprise service buses of the suppliers and, based on the results, new generic management services and buses were designed.
8. We have studied and analysed the proposed SOA development roadmaps and have accordingly come up with a proposal for Hungarian developments.

The results and products of the project

• Compilation of pilot applications (for public administration and banks) from SOA systems.

• Testbed for assessing the interoperability of SOA and WS (web service) based systems.

• Development of application-independent XSD, WSDL and BPEL code generator software from UML model.

• Publications: 1 lecture at an international conference, 2 lectures at conferences in Hungary, 2 MSc theses, 5 BSc theses

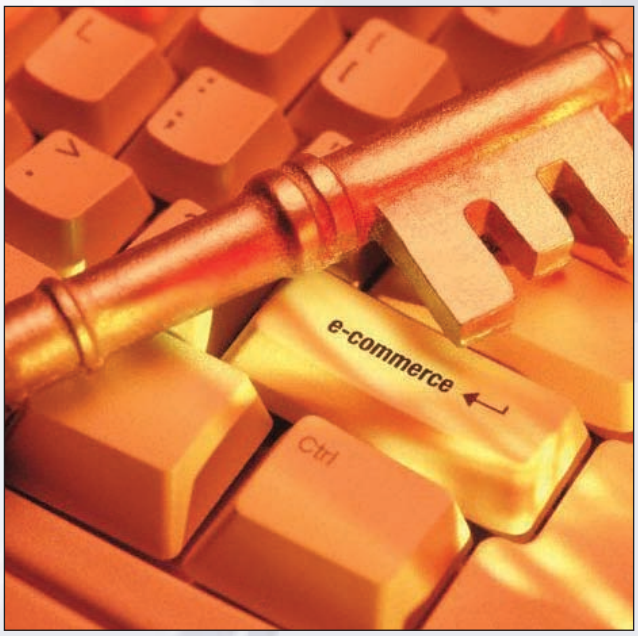
3. e-SECURITY DEVELOPMENT DIRECTION

Project director: Dr. Zoltán László professor, MSc in Electrical Engineering
Research area: software engineering, metaprogramming, development of distributed object oriented systems, software engineering education
Publications: books: 1, lecture notes: 6, journal papers: 7, conference papers: 48
Important research and industrial projects: GVOP, IKTA, TÉT, ITEM, IST, TEMPUS projects
Awards: Award for Outstanding Innovation, KPMG professorial scholarship, HP professorial scholarship.

As one of the most rapidly developing disciplines these days, information technology plays a significant role in both the operations of society and the economy, and in managing their operating efficiencies. The continuous, exponential growth of computing/storage capacity of hardware, and the drastic increase in network bandwidth enable the solving problems that once seemed to be insurmountable, due to technical limitations. However, it can be inferred that there is more to information technology on its current technical, technological level than what is exploited by creating and operating complex, highly complicated systems affecting society and economics (e.g. e-government, distribution, intelligent transport and logistics, meteorology, simulation and animation, process-, organization and decision support systems, just to name a few). This situation has been confirmed outside Hungary as well. International studies show that only a small percentage of complex IT projects can be considered successful, and the exaggerated expectations towards the sector have decreased over the last decade. This is mostly due to the fact that the security and quality of an IT system is often insufficient, and protection tools and techniques are cumbersome and difficult to manage. System downtimes result in a lack of essential functionalities and data loss, while security holes make users vulnerable. There is not sufficient support available for secure operation, connection points linking different systems are missing, and simple modifications in the application field can only be realised through complex development in the implementation field.

The more IT systems dominate every aspect of life, the more IT security comes to the forefront. International standards and regulations are created to classify systems and to certify compliance with requirements (e.g. Common Criteria), with Hungary acknowledging the efforts and aiming to employ these initiatives (e.g. MIBÉTS). Alongside the technical level approaches, organisational level approaches are becoming increasingly (COBIT, BS7799) accepted. A similar tendency can be experienced in terms of quality and quality assurance, where alongside the ISO there is an increasing demand for CMM based certifications.

The ultimate purpose of the programme was to create an IT security and quality assessment laboratory which by the end of the project could become an IT certification laboratory. Besides, it was also meant ensure that IT security assessment methods should gain ground in Hungary. This latter can contribute to the development of a Hungarian as-



sessment scheme and can prepare the Hungarian products for internationally recognized certification procedures. This results in a considerable cost reduction for Hungarian enterprises, as if they plan to have their products or services certified for the Hungarian market only, they will have an inexpensive solution at hand. The thorough preparation, on the other hand, gives rise to substantial saving in case of international certification. Our particular research topics included analysis of new threats, techniques of identification and attestation, secure payment protocols, audit methodologies and their computerized support, as well as determination of quality attributes, metrics and measurement methods of products, resources and processes.

Developments were conducted within the frameworks of four application projects that were initiated as per the innovation needs of the consortium partners. In spite of the fact that we could not launch a joint enterprise with our partner, SQI Kft., we have achieved our professional and R&D aims within the quality laboratory project. In collaboration with SQI Kft. we have developed and mutually exploited the software application supporting CMMI audit and have drafted the framework of an ISO 9126 compliant product-based audit. Using the competencies acquired in the course of the project, the laboratory workgroup intends to carry on its activity in the field of assessing applications handling open document format in collaboration with the Hungarian universities ELTE and SZTE, as well as its as well as its industrial partners. Two projects were related with developments carried out at Balabit Kft. The objective of one of the projects was to prepare the successfully distributed Zorp v3.2 firewall for CC EAL4+ level pre-evaluation. In accomplishing this end, the researchers of the Knowledge Centre's laboratory gained experience in CC methodology application, while at the same time they also proved to be capable of providing a service in this field. Within the frameworks of the other project the popular and much renowned, flexible and scalable open-source system logging program, syslog-ng was to be enhanced and made into a marketable product. This project resulted in a full logging infrastructure based on the open industrial standards of the Internet, thus enabling connection with other systems, e.g. supervision, analysing or archiving systems. Another project aimed at the development and enhancement of high-level security, virtually closed networks, and ultimately, the creation of a marketable product. This project is carried out in partnership with Navayo Research Kft., formerly known as Secfone, and is based on the patented Manageable Virtual Closed Network protocol and secbox device, which provides network access. In the course of the project we have prepared the Common Criteria methodology level EAL2+ compliant security documents. We have carried out the vulnerability examination of 'secbox desktop 5', the outcome of our enhancements, and we went on to perform the assessment of the product itself. Our partner has been successful in selling the product in vast numbers in Japan and the United States of America. We have also developed the reference implementation of a secbox to be embedded in next generation mobile phone devices. The project has also resulted in a number of 'by-products' that can be readily used in practice (automated test system, centralised MVCN-level logging, high-security fingerprint reader) and are therefore likely to be made use of in the future.

3.1 IT quality laboratory (1.2, 3.4 subtask)

e-Security development direction

Project manager: Dr. Zoltán László

Objectives

The quality of software is a challenging problem in IT industry, both from the perspective of quality assurance and measurement. Software quality measurement can be interpreted from the viewpoint of either the product or the process in which the software is applied. Within the scope of the current project, BME $(IT)^2$ is aiming to set up a laboratory providing services in both product and process-based quality control and quality assurance. The aim of the present project is to have BME $(IT)^2$ and its employees cooperate with software vendors while providing consulting services and assistance in creating the quality profile of the company, and in assessing software characteristics using quality standards. In order to support the process based SCAMPI quality auditing process, BME $(IT)^2$ is implementing a software to record CMMI model requirements and their completion.

In the field of product-based quality control we are aiming to create detailed guidelines for measuring several quality metrics defined by ISO 9126, and to create a framework where there measurements can be planned and maintained. Using these tools we are also aiming to solve a specific measurement task.

Project members are aiming to achieve remarkable results - supported and documented by several publications - in terms of the technological aspects of software quality in the fields of model-based software development and aspect-oriented programming.

Primary goal of the project is to involve students and young researchers in the project to help prepare the software product mentioned above.

Summary of the activities

In the first work phase based on the ISO 9126 standard - and also the Goal/Question/Metric (GQM) methodology, adopted as a definition for the certification process - a general control engineering software-related quality profile was elaborated. As for the NAT (National Accreditation Board) accreditation, a first version of the accreditation scenario was created. The system specification and the prototype of the CMMI audit supporting software (CMMI Assistant) were completed before the deadline and - within the frame of a dedicated contract - handed over to SQI Pty Ltd., where the prototype was installed and functionally tested.

Meantime, a model-based and aspect-oriented code generation technique was elaborated and published.

In the second work phase detailed guidelines and scenarios for measuring several metrics defined in ISO 9126, and a framework where these measurements could be planned and maintained were created. The framework defines the general processes (handled on a measurement guidebook level) of the quality measurement system, and also demonstrates how measurement processes can be customised using measurement instructions. The measurement supporting framework defines the documents and processes to be used. By elaborating the most important metrics one after another, a basic structure of the measurement system was also created. Thus, further metrics can be added to this structure in a straightforward and automatic way.

In the following step we examined how the elaborated measurement system could be introduced. In order to do this, the mapping of the development company's internal processes to the ISO 12207 life cycle standard, and the assignment of ISO 9126 metrics to the ISO 12207 phases seemed to be inevitable. After investigating how frequently the ISO 9126 metrics tend to affect these phases, interview-questionnaires were created for each phase. In addition to the analysis of metrics, the processing of further standards (ISO 14598 series, ISO 25000, ISO 15939) was started, as well.

The elaborated measurement system was moved into practice through two tasks.

The SPC v5.5 software created by the HNS company was thoroughly examined, and a detailed measurement guideline was compiled that took into consideration the following metrics.

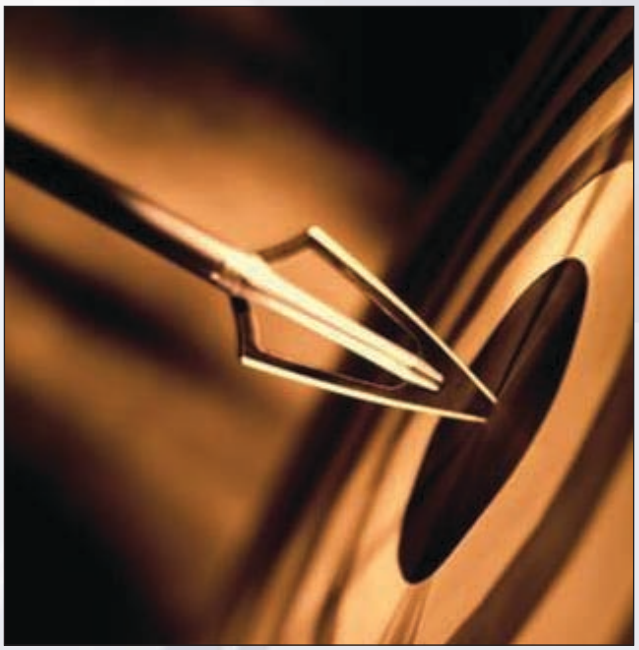
- E.5.3.1 Change success ratio
- E/I.1.1.4 Functional specification stability
- E.5.1.3 Failure analysis capability
- E.5.1.2 Diagnostic function support

In spite of the fact that the above selection included metrics that could be measured without close cooperation with the developers, the company claimed to be too occupied with other engagements and therefore postponed the instalment of these measurements into the system.

The second practical task was to measure the following characteristics of the secbox software developed within the scope of the „3.3 Virtually closed networks" project.

- E.8.1.1.3. Functional implementation coverage
- E.8.1.4.1. Access auditability
- E.8.5.1.1. Audit trail capability

Unfortunately, the planned measurement could be carried out only partially in the second work stage. One reason for this delay is that current developments are continuously changing the secbox software, thus making the software unstable. On the other hand, the delay is due to the fact that the complexity of the communication and testing system required to fulfil this task was highly underestimated.



The resulting jwebunit-based test system proved to be highly platform-dependent with basically no robustness. In the third work phase jwebunit was replaced with the similar (web application testing) Selenium (http://selenium.openqa.org) system. By extending and adding test programs to Selenium an automatic tester was created which was adopted by the secbox developers in 2008 October.

Alongside with the definition of formal-model based development methodologies, a new version of the aspect-based code generator was created, and verified using a real-life task. The input consisted of the UML model of a software system and the code of the software itself (Java, Java beans, JSP, HTML templates). During the problem-solving phase based on aspect definitions, the code was recreated from the model by intuitively recognising different aspects. Our new programming technique for traversing models was introduced in a presentation at the IADIS Applied Computing conference, Salamanca, Spain.

We have also attempted to extend formal modelling to functional programming languages. A prototype of an Erlang refactoring tool was created, while putting an emphasis on the application of ready-made components and technologies. The source code was modelled with an annotated abstract syntax tree represented in XML. Due to this choice of technology there were several tools available for model transformation and visualisation. These results were discussed at the IASTED Software Engineering and Applications conference in Cambridge, USA.

The prototype of the CMMI_Assistant program was handed over for use to SQI Pty.Ltd. at the end of the first work stage. In the second work stage the program errors are continuously corrected, and also some minor modifications were carried out. SQI Pty.Ltd. used the prototype as a pilot during the audits carried out. For the program use, SQI Pty.Ltd. is paying a fee according to the arrangement.

A feasibility study corresponding to the aims of the quality and security laboratory was also created, that summarises the most commonly used quality certification processes, and - using a survey - illustrates the connection between supply and demand in the quality certification market. Based on the results of this survey the study concludes by making a suggestion of creating a vendor-independent IT security and quality assessment laboratory within the scope of BME $(IT)^2$, by defining main goals to be achieved and activity roles to be created.

As part of the appearance of BME $(IT)^2$ the project was introduced at the CEBIT in 2007.

According to the plans the project was closed at the end of the second work stage. However, in the third work stage – alongside with secbox testing and measurements – the Quality Laboratory staff carried on performing their tasks in the fields of software quality model analysis and applicability, and in the field of software product characteristic measurement by testing. The results of these researches were published at local and international conferences, and various periodicals. Further goal is to provide process- and product-based software quality assessment for open document format (ODF) applications. The task is to create a quality assurance schema based on code analysis results – in case of internal metrics; or based on ISO 9126 by defining external metrics. Capitalizing on the test systems and frameworks created by the project staff their further aim is to analyze the “in use” quality attributes of ODF format creating applications, as well.

The results and products of the project

- Summary of the Goal/ Question/Metric Method - study
- Description of the external, internal and in-use metrics of the ISO 9126 - specification
- Quality profile pattern for an industrial software - specification
- Quality handbook
- Software (CMMI Assistant), supporting CMMI auditing - system definition, design and implementation plan, user documentation, software (prototype)
- Model based aspect oriented code generator (technology)
- The most important achievement of project was that a laboratory providing service in quality control and quality assurance both for software product and development technology was set up at the $(IT)^2$.
- The general framework for measuring quality metrics was modified based on the ISO 12207 standard.
- A list of interview questions regarding the internal development methods of software development companies.
- A testing framework program built on jwebunit for testing secbox.
- A Selenium-based test framework for testing secbox.
- An aspect-oriented code-generation technology based generator program (prototype).
- An Erlang refactoring program (prototype).
- IT Security and Quality Laboratory - feasibility study.

3.2 Evaluation of Firewalls (subtask 3.6)

e-Security development direction

Project manager: Áron Szabó M. Sc. in Electrical Engineering (BME), BME Knowledge Centre
Specialty: cryptography (PKI, XML signature, XML encryption) based solutions (e-signature, e-invoicing, e-archiving, e-market), product assessment (Common Criteria, MELASZ Ready interoperability), Web Service technology (SOA model)
Publications: 8 lectures at conferences

Our partner, BalaBit Kft. has dealt with development and service providing of network protection and network management based solutions since 1996. Zorp modular firewall and syslog-ng log manager are well-known and recognised products of BalaBit Kft. The company was also awarded an ISO 9001 certificate for their development processes in 2004.

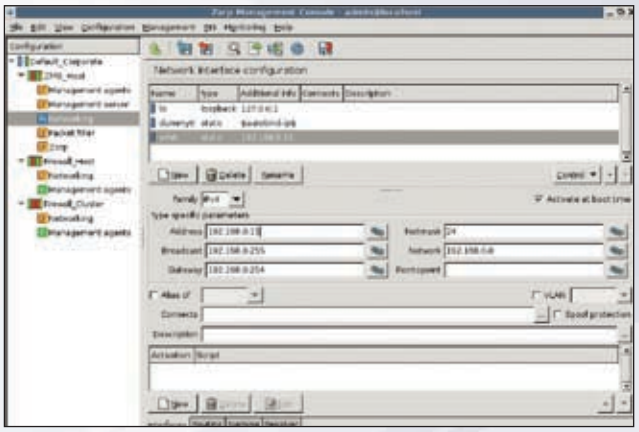
Zorp firewall is used in wide area because of its capabilities, flexibility and graphical management interface. The modular Zorp can be used in environments where other products of concurrency are not suitable. This firewall can solely provide protocol analysis and content filtering inside an SSL encrypted channel. Decision rules, permissions, denials based on information security policies of companies can be easily set because of great flexibility. Zorp was certified as ICSA "Corporate Firewall" in 2004. Zorp firewall can provide sufficient protection even in fields with very strict security policies, such as government and the banking sector. The need for product assessment from information security aspects was brought about by market competition. Zorp has not yet been evaluated, therefore BalaBit Kft. decided to get a Common Criteria EAL4+ certificate. The first step of this long and extremely costly process is the creation of a Security Target (ST) document.

The task leader of this project from our partner's side is Endre Wágner, a software engineering graduated of the University of Veszprém (whose present-day name is University of Pannonia). His wrote his degree thesis on the teaching of the scheduler of the Linux kernel by means of neuron networks. He participated in the implementation of network IT security rules of Magyar Telekom in 1997, then he became the IT security manager of T-Systems Dataware in 2000. Since 2003 he has been the technical director of BalaBit Kft. In 2004 he got a CISA certificate from ISACA.

Objectives

The Common Criteria (CC) is the most honoured technology-based IT security related assessment methodology. This methodology was proposed as a standard and was issued as ISO/IEC 15408 by the international standardisation organization. The Common Criteria certificates of products are basically expected by public services, banks where IT security requirements are high.

The market analysis of our partner showed that some of the rivals of Zorp firewall have also got Common Criteria certificates. Seeing the results of these researches, BalaBit Kft. aimed to get EAL4+ level of Common Criteria pre-evaluation of Zorp within the frameworks of this (IT)2 project. EAL4+ assessment level was chosen because getting a certificate at a lower level would not make up leeway of Zorp, and also a higher level would have much higher cost that could not been financed in this project.
Hungary joined Common Criteria certificate recognition arrangement on in 2003, but it still has no right to issue any certificate, therefore we can only provide a pre-assessment instead of a real one. There are a limited number of specialists with a thorough knowledge of Com-



mon Criteria who could prepare a product for assessment. However, the laboratory of the Knowledge Centre is experienced in the assessment of Common Criteria projects with some cryptography based solutions involved.
In this project - which has only one work phase of one year period - BME (IT)^2 and BalaBit Kft. provide together the documents and tests needed for the commencement of a real assessment.

Summary of the activities

This project was started in the second work year of BME (IT)^2 , so it does not have any antecedents. It is indirectly connected with the preparation of Navayo secbox CE100 - within the „Virtually closed networks" project of the Knowledge Centre - for the Common Criteria EAL2 qualification. The results of the current project also serve as important experience for starting other services in the future at the IT security laboratory, such as the preparation for Common Criteria evaluation and certification, and a specific phase of this, vulnerability testing („Ethical Hacking").

Using experience gained from similar jobs, we created the project plan, which can be found in the Deed of Foundation. Before the initial steps were taken, the project members of the Knowledge Centre involved in the project participated in the „BalaBit Certified Zorp Associate" course, in order for them to have the sufficient knowledge to examine the product extensively. After this course, the first task was to prepare the Security Target, a document containing the functionality details of the product. The existing documents of the industrial partner (BalaBit Development Process Definitions, BalaBit Development Infrastructure, BalaBit Coding Conventions, Zorp Test Documentation, Source in TLA, Zorp Administrator's Guide, Zorp Reference Guide, Zorp Installation Guide, BalaBit General Policy) were looked at, and after further examinations the list of missing documents was assembled. After examining the public articles about similar evaluations of market rivals, the extension of the details of the documentations became reasonable. Accordingly, the group of functional expectations to be examined was broadened to the 19 proxy modules of the firewall (Finger, FTP, HTTP, IMAP, LDAP, LP, MIME, NNTP, Plug, POP3, PSSL, RADIUS, RSH, SIP, SMTP, SSH, Telnet, TFTP, Whois), and was put into the Security Target. Consequently, the 19 proxy modules had to be involved in the functional testing besides the Zorp core. The functional testing was executed in a testing environment created at Balabit Kft. The suite of functional test cases was assembled by collecting and sorting existing test cases - primarily connected to the proxy, a dataflow-analyser and protocol element verifier - and creating the missing ones.

The vulnerability tests of the product were executed by the Knowledge Centre IT security laboratory „Ethical Hacking" group. To accomplish EAL4+ level, besides „black box" penetration testing, source code analysis of the security functions was also necessary (for example utilising source code analyser software). According to the Common Criteria methodology, medium „hacker" knowledge and public („exploit") databases were applied during the penetration tests, which were to prove the protection of the product. Based on the existing documents the other manuals - with Common Criteria compatible level and syllabus - were compiled. These documents introduce the architecture and the subsystems, give details of their functionality, and contain the part of the source code. The installation, setup manual and the user guide were written as well. The life cycle document of the product was created including the support, the ways of error reporting, handling and reparation and the shipment conditions. Various reports, analysis and records were attached to certify that the depth and the coverage of the tests meet the requirements and that the analysis of the functionality, vulnerability testing and penetration testing is completed.

According to the tests and documentations done within the project, the evaluation and certification procedure can be started at an institution with appropriate authorities (for example at the Bundesamt für Sicherheit in der Informationstechnik in Germany).

The preparation for the CC evaluation was completed during the project, as a one-time task. However, the experiences gained during the work enables us to perform similar projects in the future.

The results and products of the project

Preparation to Common Criteria evaluation

- Security Target (ST), general description of product, functional and assurance requirements, security objectives, threats, assumptions, organisational security policies and correspondences;
- ADV_ARC.1, about security architecture;
- ADV_FSP.4, about functional specification;
- ADV_IMP.1, about implementation representation;
- ADV_TDS.3, about TOE design;
- AGD_OPE.1, about operational user guidance;
- AGD_PRE.1, about preparative procedures;
- ALC_CMC.4, about configuration management capabilities;
- ALC_CMS.4, about configuration management scope;
- ALC_DEL.1, about delivery;
- ALC_DVS.1, about development security;
- ALC_FLR.1, about flaw remediation;
- ALC_LCD.1, about life-cycle definition;
- ALC_TAT.1, about tools and techniques;
- ATE_COV.2, about coverage of tests;
- ATE_DPT.2, about depth of tests;
- ATE_FUN.1, about functional tests;
- AVA_VAN.3, about vulnerability analysis.

3.3 Log-gathering and analysis (3.6 subtask)

e-Security development direction

Project manager: Szabolcs Szigeti

Our industrial partner, Balabit Ltd., has been developing network security and network management tools and services since 1996. Some of their most well-known and acclaimed products are the Zorp modular firewall and syslog-ng. Zorp is popular due to its flexible features and graphical management console.

Syslog-ng was created as a replacement to the original syslog tool. It has gained tremendous popularity in free and open source communities. The goal of this project is to create a general log-gathering hardware-software infrastructure framework based on syslog-ng.

The industrial partner's project leader is Csaba Major. He graduated as a computer engineer at Miskolc University in 2000. Since then he has been working at Balabit as a systems engineer and leading systems engineer. He is currently working as an IT security consultant, specialised in Linux, firewalls in general and specifically the Zorp modular firewall. He is a certified Zorp engineer.

Objectives

Balabit's popular syslog-ng tool has been available for a long time. There is market demand for comprehensive logging frameworks, and this software is an excellent foundation for such a product. The project is aimed at developing a software product that could be used to gather and store the log events generated by large IT systems, networks, server rooms, etc. The system should have a hierarchical structure to forward the events from different sources to the central log storage.
The result of this project will be a logging infrastructure, which is based on industry standards, and thus will be able to interface to other systems performing tasks such as management, analysis, and archiving. This would provide more flexibility for the user.

Summary of the activities

In the first period, the project was started. The project goals were established, and the project infrastructure was created. At the start of the design phase, the full system specification was laid down. Based on this specification, we created the whole system design. After that, the project advanced to the implementation phase.

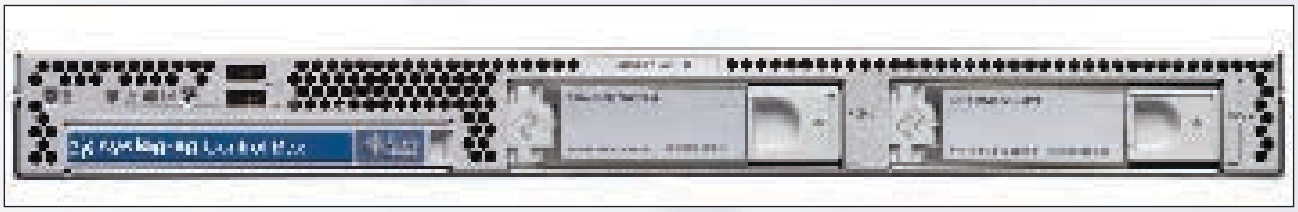
The goal was to create the two main system parts, the central management console and the log gathering hardware/software component (the relay). To achieve this goal, three components had to be developed:

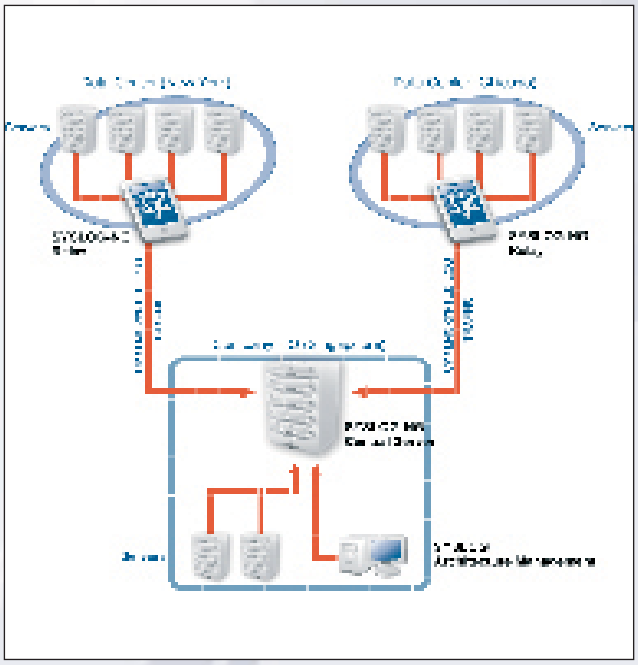
1. The firmware for the relay. It is based on the Linux operating system, with web based software for communicating with the management system. Main parts of the development were the solution for downloading the configuration and updates and the method for controlling the different components of the relay. The XML schemas for transferring configuration and the processing modules were created.

2. The configuration database and its management system for the relays. Because of the large number of relays, scalability was very important. The management database is based on the hierarchy of the relays. The management module handles the database, and transfers configuration and access control information to the relays.

3. Central management console user interface, which is connected to the management database. There were three important points to take into account during the design: usability, scalability for thousands of relays, similar look-and-feel to other Balabit products and web-browser based solution. The solutions used for Balabit's Shell Control Box product was used. With the advanced AJAX technology a user-friendly user interface was developed.

Because the project ended in the second stage, all tasks planned for the project had to be finished during this time. Engineering and marketing tasks were carried out concurrently. The following engineering tasks were completed during this period:
1. The hardware configurations for the management console and the log-gathering relays were specified. Plans were made to sell the product as an appliance, with the software pre-installed. The relays are currently running on embedded PCs (with no moving parts and with flash-storage). Choosing the configuration was left to the end of the project, because due to the fast development of hardware, the market supply of necessary devices frequently changes considerably.



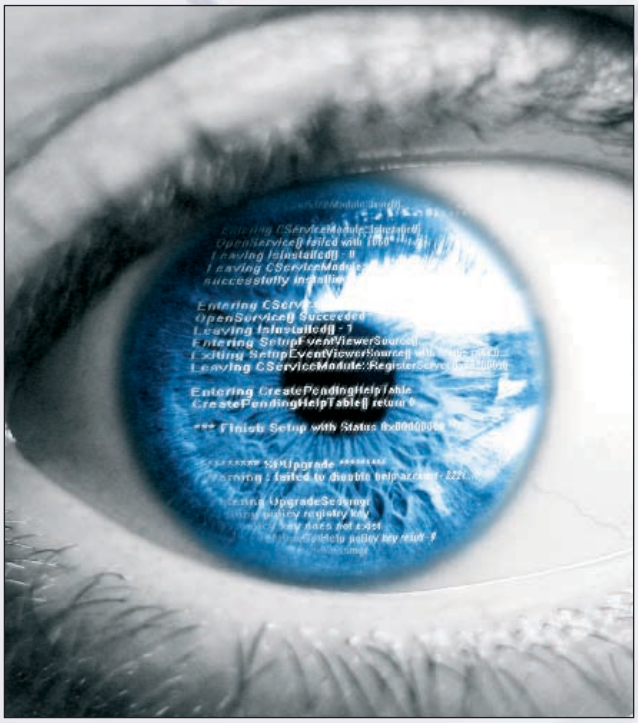


2. The modules of the prototype were integrated into a real-world environment. As opposed to the prototype, the product has to work in in a real environment on real hardware. The development environment was very different from this physical environment. Therefore, the separate modules had to be integrated to fulfil the specific requirements of this environment.

2. Testing. A test-bed network was set up at the industrial partner's lab, where the load and communications parameters of the real network environment could be simulated.

3.The graphical user interface had to be enhanced. This is because during the timeframe of this project, another Balabit product, Shell Control Box (SCB), was released, and the look-and-feel of syslog-ng had to be changed to match that of SCB in order to obtain uniform appearance.

4. Results were documented.



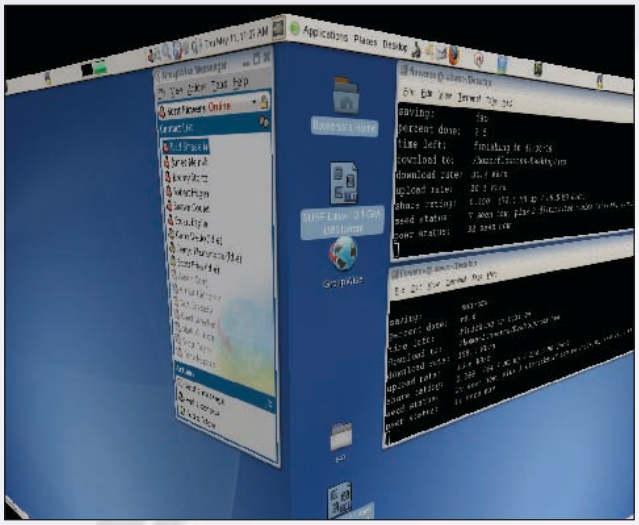
The following tasks were carried out for market release.

1. The product was presented to the professional community. One of the most important presentations was given at CeBIT 2007. Both Balabit and (IT)^2 had their own booths at the exhibition. This way, the project could be presented from two viewpoints: industry and academia. Since syslog-ng was created in a way that allows it to interface to other systems, it was important to target prospective partners.

2. Marketing materials were produced and the product appeared on Balabit's site, at http://www.balabit.hu/network-security/syslog-ng/.

3. Pricing and licensing policies were created with the industry partner.

The technology developed during the project has a considerable potential for growth, it satisfies an existing market demand. Thus further development is expected in the direction of integration with other tools, analysis ability and other.



The results and products of the project

- Project organization and infrastructure.
- Requirement specification.
- System-design.
- Central management module (software component of the product).
- Data gathering center (software component of the product).
- Syslog-ng product.
- User documentation.
- Marketing material.
- Product web-page.
- Pricing and exploitation policies.

3.4 Virtually closed networks (subtask 3.5)

e-Security development direction

Project manager: László Bacsa BA in Economics and graduating in Master of Business Administration (specialized in fiscal economics and info communications).
Director of innovation and marketing at BME (IT)², project manager at BME Centre of IT.
Fields of interest: innovation management; planning and coordination of projects; international relations; communications, marketing; strategic planning, consulting.
Publications: 2 book chapters, 4 publications and 8 conferences

Our consortium partner Navayo Research Ltd. – formerly known as Secfone Ltd. – started its research into Manageable Virtual Closed Network (MVCN) protocol in 2004. Besides patenting the MVCN protocol, the network access hardware by the name secbox was also developed. Navayo's mission is to enhance the functionality and usability of services based on MVCN as well as to develop more MVCN equipment. Hence, Navayo does research and development in specific target areas (mobile communication, video transfer, IP based voice transfer) to integrate the MVCN protocol. Their business activity covers the production of products that were developed, their introduction to domestic and international markets, as well as related sales and marketing. The industrial partner's supervisor is Mr. János Zelenák IT expert; process developer and IT lecturer.

He pursued his studies at the University of Szeged, he has been working in IT for 19 years; through his companies he has been working on several development projects initiated by IBM since 1997. His area of specialization is IP security technology.

Objectives

In these days, the freedom of Internet raises critical security questions. In terms of security, the control and the administration of communication over the Internet can only be ensured with expensive and particular solutions. The developments aim at creating a cost-effective and efficient alternative, rendering secure communication possible for small and medium sized enterprises, as well as for households and individuals. There is considerable market demand for a VoIP gateway capable of cooperating with secbox devices, as well as managing and connecting a VoIP telephone network to ISDN/PSTN/VoIP/MVCN networks. Our additional aim is to create a secure, broadband virtually closed network and to apply the technology in the next generation mobile environment.

Summary of the activities in previous work stages

The task of the workgroup for the preparation of the Common Criteria (CC) methodology was to compile the Security Target (ST) documentation pursuant to the AEL 2+ security level. At the suggestion of the German IABG (Industrieanlagen-Betriebsgesellschaft GmbH), the document was revised to be in accordance with the CC v3.1 recommendations.
In the R&D and Innovation Centre of BME (IT)² we set up an Asterisk - software based telephone sub exchange – test system. We have expanded the functionality of the Asterisk test system, creating an MVCN-Asterisk PBX product. The base system now contains a Graphical User Interface, which is a convenient interface for the system operators. We have finished and completely integrated a VoIP protocol controller /SIP conntrack/ module, which can provide seamless cooperation with an MVCN/Asterisk secure PBX.
Besides the automatic test system, we completed a testbed /"secbox wall"/ at the Navayo Ltd HQ using 100 secbox devices, to provide a test environment both for the hardware itself and for the functional and performance testing.
As a by-product of the project a centralized logging system has been completed. It is able to log all of the running parameters of all registered secbox devices in a centralized database. This application was useful for MVCN system level tests.
After several sorts of measurements and examinations, on the basis of the analyses, we determined the bottleneck of the implementation and after it was fixed, the throughput of secbox device almost trebled (3Mbit/sec).
The preparation and porting of the MVCN technology to the next generation mobile applications was started by summing up the possible solutions. We have analysed the operating systems of the present mobile devices in the terms of MVCN protocol and technology application. On the basis of that, we have chosen the Linux operating system, because using the Linux implementation of Navayo Research Ltd. gives an efficient development opportunity.

We completed a prototype, to prove the MVCN real-time capabilities by providing an MVCN endpoint in a next generation mobile environment. We had to transform the software of the MVCN endpoint to a version that is hardware and platform independent, which can be used on other Linux-based devices with the appropriate network drivers. We have designed a new Graphical User Interface for the mobile device, considering the limited resources available on a mobile device (small screen, limited bandwidth, etc.), to provide a User Interface.

The requirements of the next generation, broadband secbox device was to increase the current throughput of roughly 3Mbps to one exceeding 50Mbps, while also maintaining the security level. The development included the hardware and software design, creation of a prototype and the software implementation. The first step was to design the hardware (block diagram, PCB design) and based on the hardware, we developed the drivers and the operating system. The prototype was made by MSC Scotland Ltd. We have "revived" the prototype using the completed drivers and operating system. After the identification of some minor hardware design problems, we fulfilled the requirements and using the MVCN application layer we achieved a throughput of more than 70 Mbps.

Our industrial partner's product, the secbox device reached the latest phase of the development, the beta phase. We supplied some potential partners (customers) with demo secbox devices. We have presented the secbox device at different exhibitions and conferences. Relevant events: CeBit (Hannover), Systems (Munich), IT Gartner Channel Vision (Miami and California), and the 12th Industrial Communication Conference (Blomberg).

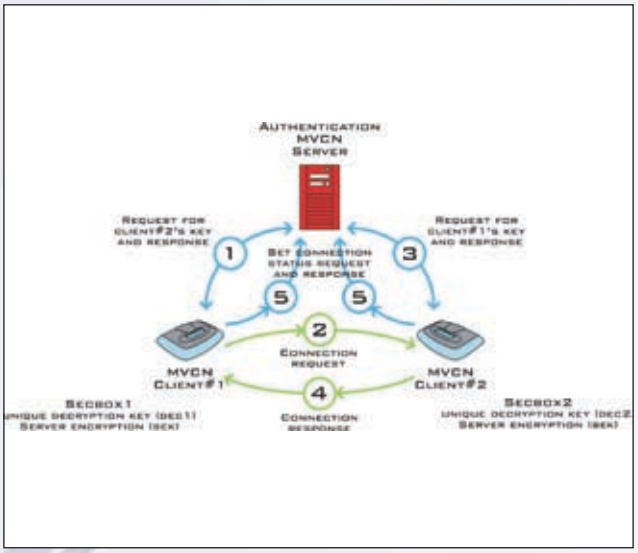
Summary of the activities in the third work stages

The sale of „secbox desktop 5" product, completed in the previous year, has started. Massive sales were achieved in Germany, Japan, Slovenia and the United States, amounting to several hundreds of units. The product was presented at several exhibitions and conferences:

1. CeBIT (Hannover, Germany)
2. Datamix Gitex (Dubai, UAE)
3. IT Gartner (Texas, USA)
4. ST Electronics (Singapore)

A number of publications and presentations were made about the operation of MVCN in Hungary and also in Japan and Germany.

Continuing the previous work stage, we have finished the SIP conntrack module for the secbox device. With the module it has become possible to make a VoIP call through the secbox devices under the supervision of Asterisk PBX. In the next step the task was to design and produce a special SIP proxy. The SIP proxy ensures a direct (peer-to-peer) VoIP connection among the secbox devices without any telephone exchange. The module was produced as planned, and was integrated into the



device for testing.

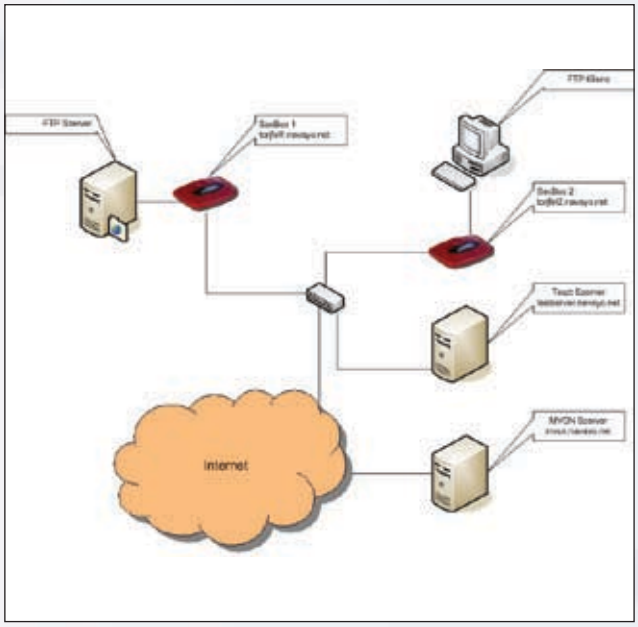
The previously used Atmel "sweeping-sensor" fingerprint-detector subsystem could not meet the Japanese market demands, therefore in devices that are produced for this target market, the sensors of Fujitsu MBF were implemented. For adequate operation, this sensor needs different settings than the previously used one. The necessary measurements, fine-tuning and tests were carried out. The reports confirm the smooth operation of the device and it has a much better recognition accuracy than the prior one.

The performance of the MVCN network's endpoints is limited because of the hardware's capacity. An obvious solution would be paralleling the devices. Because of the MVCN network's security, this solution is not a trivial challenge. A feasibility study was carried out to on how this could be resolved. After analysing the study, Navayo Research Ltd chose to replicate the secbox devices, which has been performed.

The vulnerability audit of the "secbox desktop 5" was finished in the security laboratory of BME (IT)[2]. Minor security problems have emerged, but remarkable, critical

security flaws were not discovered during the audit. An executive summary has been given about the audit. A hacker competition was organised by the BME (IT)[2] and the Navayo Research Ltd. for IT engineering students at BME. The objective of the competition was to bug and to decode the communication of the secbox devices over the Internet. No-one from among the more than 30 students could achieve the aim, as they could not find or exploit any security hole in the system.
The development of the automatic test system has been continued, involving more students. The framework's development has been finished. The system has been extended with the functions of Selenium framework which enable easy control through the graphical interface. We have processed the test cases provided by Navayo Research Ltd. and the system has been delivered.

The porting of the MVCN technology to the next generation mobile devices was continued. We have integrated



the MVCN modules (kernels, applications) into the ROAD S101 device. After converting and implanting the chosen SIP client secure VoIP calls can be placed on the device. Since the device operates as an MVCN endpoint, it becomes possible to produce a simplified "mobile secbox". The previous and completed interface of the device has been extended with a graphical interface, which enables simple and easy management of secure calls with the possibility of configuring settings on the interface. The produced system in the ROAD S101 complies with the requirements defined in the specification. Hence, the next generation mobile reference-implementation of the secbox is finished.

The results and products of the project

- MVCN - Asterisk PBX system (product).
  - o Integrating an MVCN endpoint into the PBX system.
  - o Selection of the Graphical User Interface and porting to the system.
  - o Interfacing the conntrack module to the secbox.
  - o Producing SIP proxy for the secbox ensuring peer-to-peer connections.

- MBF 200 sweeping-sensor fingerprint reader subsystem.
  - o Design, implementation, functional testing, fine-tuning and testing.

- Next generation secbox (prototype).
  - o Hardware design
  - o Operating system, device driver design and implementation.
  - o secbox application porting to the new device.
  - o Creating the prototype (MSC Scotland Ltd.).
  - o Testing, debugging.

- Preparation of Common Criteria Security Target based on the CC v3.1

- secbox device functional automatic testing.
  - o Creation of framework.
  - o Processed the test cases provided by Navayo Research Ltd.

- Vulnerability audit of "secbox desktop 5".

- Next generation MVCN endpoint (prototype)
  - o Making of the prototype, functional testing in mobile environment.
  - o Transformation of the MVCN endpoint into a platform independent application.
  - o Designing a graphical user interface, MVCN endpoint extensions to allow connection with GUI
  - o Implementation of the Graphical User Interface
  - o MVCN endpoint functional testing on the device

- Parallel operation of secbox.
  - o Completing the study.
  - o Implementation of the secbox device replication model.

4. GRID AND IT SECURITY LABORATORY DIRECTION

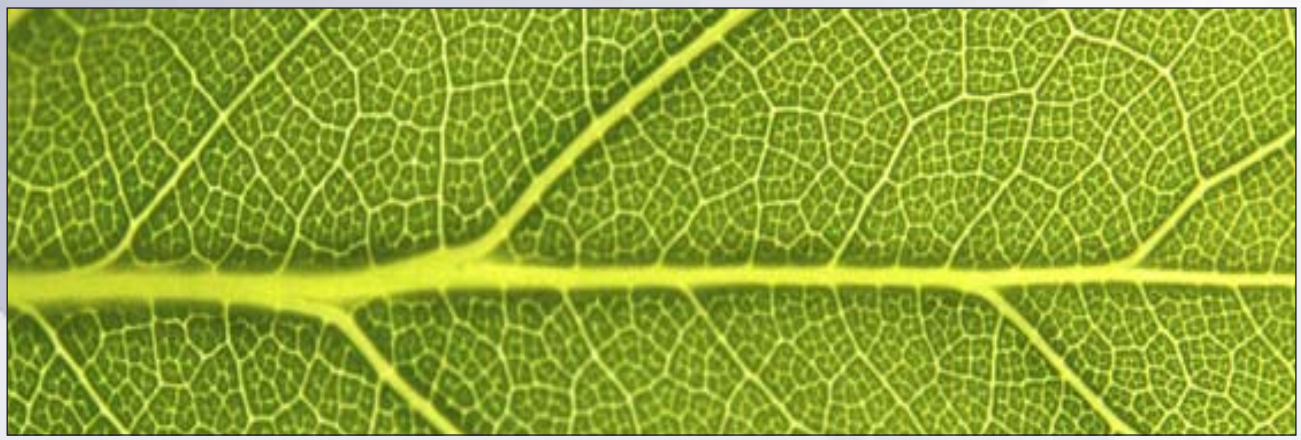
Project director: Dr. Imre Szeberényi, PhD, associate professor, MSc in Electrical Engineering, BME Department of Control Engineering and Information Technology, Centre for Information Technology
Fields of interest: Parallel and distributed systems, Grid systems, operating system, embedded systems, inter-process communications, protocols, IT security
Publications: 2 books, 19 reviewed articles, 57 lectures at conferences.
Membership: Member of the John von Neumann Computer Society, Director of the Hungarian Competence Centre (MGKK)
Major industrial and research projects: Foundations of the Hungarian IT resource system (Grid) project (National Research and Development Programs), Enabling Grids for E-sciencE project (EU FP6), User-oriented unification of Hungarian SuperGrid and ClusterGrid systems (IKTA), Implementation of ENUM procedure based services (GVOP), Development of IT security expert's studies, Review of MIBÉTS materials (IHM, NT).

On developing global distributed IT systems, we must consider security solutions, resource scheduling and data distribution even more thorough fully than with ordinary systems. The Grid and Security Laboratory project group deals with problems that our industrial partners face and are related to sizeable IT systems and Grid systems application, development, security and operation.

The creation of sizeable distributed systems was (and is continuously) made possible by the sudden development of data transfer solutions. IT resources (computing and storing capacities, data) and services (search and processing services for example) become accessible on demand, giving rise to a much more efficient resource management. At first, resource sharing was mainly necessitated by academic research tasks, but nowadays this need has surpassed academic circles and industrial users are more and more eager to take advantage of the new technology. The reason why distributed systems were at first only popular in academic circles is the involvement of a vast number of researchers from various institutions in one single research task. In this cooperation, therefore, it is only natural and logical to effectively coordinate and utilise the distributed resources available at the research laboratories.

Grid research, thus, was initiated by the need to coordinate resources of a geographically widespread research, and this span off into the world-wide research. A need for distributed, dynamic, and on demand utilisation of IT resources stems from the simple realisation that for most of the users IT application services are just like other well known services. As the number of IT systems users increases, there are more and more people who are not interested in technical details of the solution at all.

Consequently, today's great challenge is to transform distributed IT systems into systems that are usage-oriented with a service approach. This task raises a number of technological problems, such as load balancing, security and identification, reliability, service quality issues, synchronisation of large scale file systems, etc.
Grid research enjoys considerable support throughout the world. Their results cannot be separated from Web technologies, in fact, the results so far can be regarded as the latest generation of the Web technology. Moreover, Web technology also enables the creation of easy-to-use user interfaces, facilitating the industrial application and propagation of the results.
The subtasks of the project group have several objectives: first, they foster industrial application of the Grid



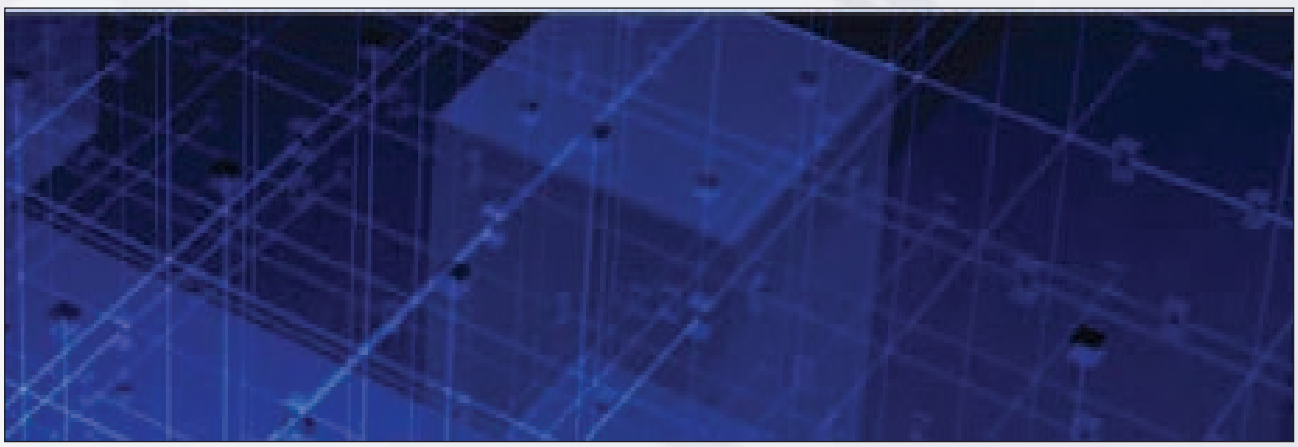
technology in industrial design tasks. Secondly, they support application of the industrial partner's scalable storage device in Grid environment, based on distributed and extended file systems. Thirdly, they enable us to prepare the laboratory for sizeable IT systems assessment, define its methodology, and try it on sample assessments.

The subtask that is related to solving processing intensive design tasks aims to develop and implement an actual industrial application. The final outcome of the subtask

will be a service based on Grid infrastructure that backs up the everyday design operations of our industrial partner. This could render large trussed bridge-beam design and manufacture faster and more efficient. Connected with that, the most important objective of the third work stage was testing on real problems of the Gradient Hybrid Algorithm (GHA) and developing the algorithm. With the help of GHA, the exponential computing requirements of PHA has been decreased to a polynomial degree. The engineering motivation of implementing the former algorithm was supported by the real market demand for such an algorithm by the reinforced concrete manufacturing industry.

The objectives of the third work stage of the distributed and extended file system project was to solve the problems of synchronisation appearing with large file systems containing countless files. The new synchronisation method, what has been developed can be used for synchronisation of different kind of well known file systems not only in HP SFS environment.

The popularity of Grid systems is dwindling as a result of the lack of confidence in its security systems. Issues of security, however, are common in all IT systems. An objective scheme measuring IT security is a great challenge for developers and customers alike. Objectives of the third sub task include the establishment of a security laboratory which, in the beginning, helps solve problems of security arising in the course of BME $(IT)^2$ projects, and later on, becomes an accredited assessment laboratory. In connection with that, we have developed our Ethical hacking service, which is becoming a more and more widespread method of evaluating large IT systems protection from external attacks. Ethical hacking is an IT security assessment method in the course of which we use the tools of the hacker to empirically evaluate system defence. The methodology we developed within the project links this method with other, formal evaluation and certification methodologies (such as ISO/IEC27001:2006 [BS7799], Cobit).



4.1 Distributed, extended file systems (subtask 4.3)

Grid an IT security laboratory direction

Project manager: Dr. Imre Szeberényi

Our consortium partner HP, is the international leader in developing and producing information technology devices, solutions and services. In the first year of our cooperation, we entered into direct research partnership with the High Performance Computing department of HP Worldwide. The research and development teamwork in Grenoble (France) pays special attention to the development of scalable data storages with large capacities. One of the motivations behind the development of the HP SFS (Scalable File Share) based on the Lustre technology is the prospect of supporting high performance Grid clusters with reliable, fast and easily extendable storage devices. Dr. Gavin Brebner (M.A., MSc., PhD.), the subject expert on behalf of our partner, works as a senior technical contributor in the Advanced Development & Strategic Customer Management team of Hewlett- Packard's High Performance Computing Division. The cooperationhas helped improve existing relations. He has visited Hungary and the laboratory of CIT several times in connection with the project. Dr. Brebner previously took part in the design and development of the SFS system and now his current work and duties are closely related to the SFS and to Grid system. He leads research and development projects that help the utilization of HP SFS in Grid systems. Previously he was working in Hewlett-Packard's Central Research Laboratories in England, and prior to that, he spent many years in industry and academia, researching and developing application-specific integrated circuits.

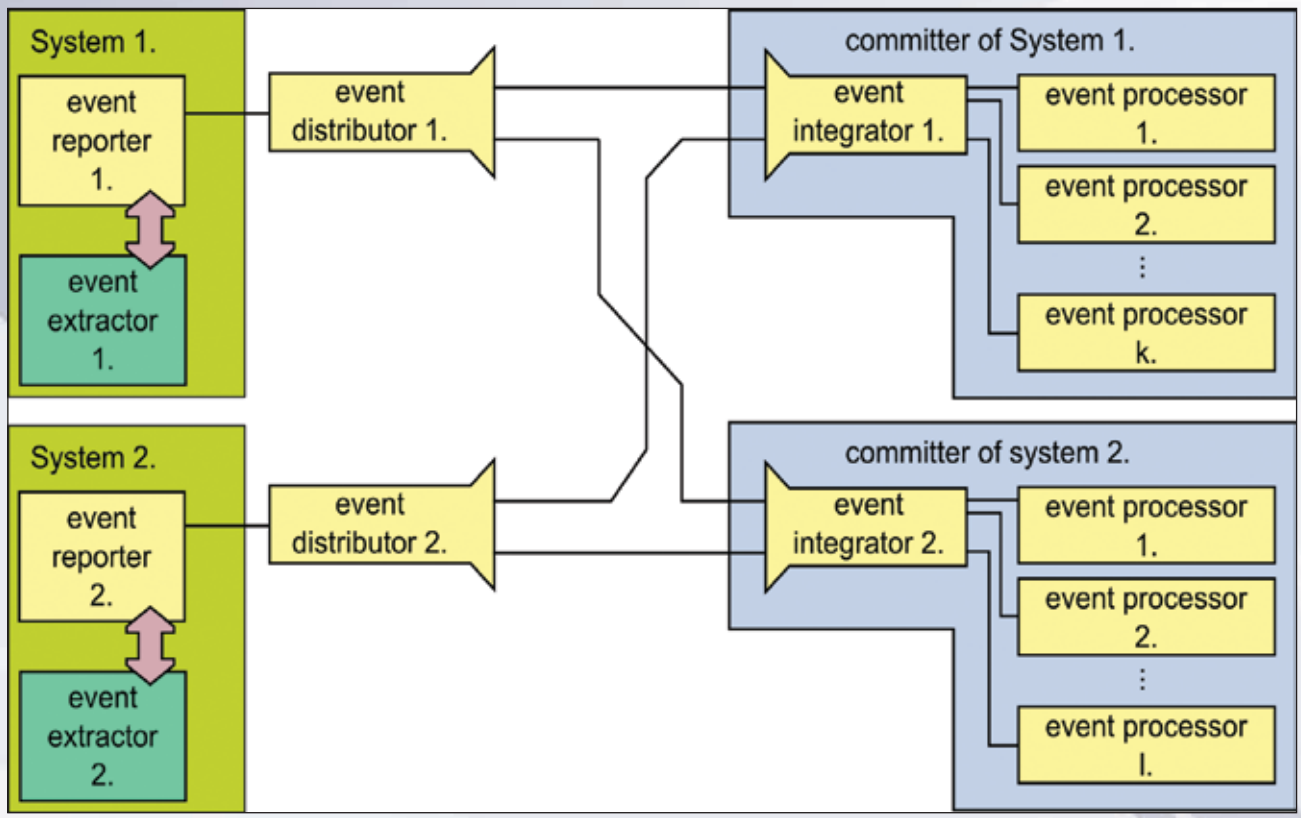
Objectives

The rapid development of network technologies made it possible to use high-capacity storages as remote resources or to combine them to attain even greater capacity. Storages like these are used, for example, at CERN to store the data of the recently started particle collider (LHC). However, the remote network connections involved can cause considerable delays due to insufficient bandwidth capacities, and make planning distributed file systems more difficult. The primary scope of the research task is the discovery and elimination of the problems caused by limited bandwidth capacities, as well as lags and network errors.
The objectives are as follows:

1. Gain access to brand new technologies and competencies, which provide current knowledge and feasibility to the region.
2. A sample HP laboratory is to be established, which may operate as an HP test laboratory in the future.
3. Support the usage of HP SFS in other industrial and/or scientific projects.
4. Design the procedures for synchronizing large file systems.
5. The long-term goal is to provide competitive storage capacities for data-intensive research.

Summary of the activities in previous work stages

The environment that the work requires was created. This task was important because this was the first HP SFS device ever to be used in Hungary and even in Central-Europe. With the cooperation of experts from HP, the appropriate SFS device was chosen and installed onsite at BME CIT, which allowed the execution of a number of performance measurements and tuning tasks. The present system provides enough space for 3 terabytes of redundant data. The clients can access this though the object-oriented Lustre technology. In the first stage of the project, we incorporated the HP SFS storage capacity into the Enabling Grids for E-sciencE (EGEE) project, with one of the goals being to provide storage and processing infrastructure for the 15 petabytes of data extracted from the Large Hadron Collider at CERN.
In the second stage we discovered problems arising from synchronising huge file systems containing a very large number of files, and developed procedures for eliminating these problems. We expected that these procedures would overcome the difficulties of existing tools and would make it possible to connect databanks at large geographical distances.
In cooperation with the research team of HP, we developed a solution with easily switchable components, which enabled our solution to be applied in systems which are not based on the Lustre technology. The draft design of the system is illustrated on Fig. XXX, which shows the synchronisation modules. The synchronisation module generates events for each relevant file system access, which is tagged by the event extractor with the appropriate information. This event is sent by the event reporter to the event distributor module which makes it available to all participating systems. The task of the event integrator is to ensure the events are ordered.
The events provided by the event extractor and integrator components makes it possible for applications located anywhere to receive notifications of the changes executed on the file system. As most event integrators are not local, but running redundantly at different points of the network, we created an event integrator which allows an authenticated component located anywhere to collect, clone, optimise and store the events temporarily or persistently.



Summary of the activities in the third work stages

The task of the third work stage is to finalize the implementation of the module designed in the second work stage, and the implementation and enhancement of the synchronization application.
On the basis of the experience gained during the testing of the prototype modules, we generalized the modules. This means that we defined the operating system interface of the extractor module and it can be connected to other networked file systems. The essence of the solution proposed is that the file system monitored and the tasks performed regarding the events can be freely substituted and combined.

The design of the system is the following:

1. The basis of the system is a standardized file system event handling system. The actions performed on the file system are intercepted at the VFS layer, and are described in a standardized, file system independent way. The events, which came into existence by slight modification of the kernel are tagged and organized by the extractor kernel module. These events are passed to the event distributor, which organizes and shares them with all the participating machines. This message handling system is independent for the type of the file system and the applied event processing.

2. The kernel with the modifications of the different file system is capable of signalling the applied changes to the system. The modification must be made to the server machines which spread the information through the message handling system. The currently supported file systems are:
- Lustre
- NFS
- Samba

3. The output of the system is a freely pluggable module, which handles the incoming events. We implemented the following three different modules:
1. List of modified files, which is ideal for creating full or incremental backups.
2. Synchronization, which is able to execute the modifications of other file systems.
3. Inotify calls: Inotify is relatively new, but widely used service of the Linux kernel, which is used by programs to receive notifications of the changes in files. Up till now, it was only possible on local file systems.

The results and products of the project

- The refined project specification.
- The installation of the hardware system.
- The analysis of the system shipped by HP.
- The establishment of the test system and laboratory.
- The integration of the SFS in the EGEE infrastructure.
- The integration of the SFS in the ClusterGrid system.
- SFS client patches for newer Linux releases.
- The redesign of the SFS client installation procedures.
- The plan of the modules of the synchronization system.
- The implementation of the synchronization modules.
- The Sequencer capable of global and local ordering of events.
- Indirect product and professional acknowledgement that BME CIT organized EGEE07, the biggest conference of Europe related to Grid technology in 2007. The seven-day conference hosted more then 600 delegates from 47 countries, and gave place for 275 professional lectures related to the application and development of Grid systems.

4.2 Industrial application of GRID systems (Subtask 4.3)

Grid an IT security laboratory direction

Project manager: Dr. Gábor Domokos Professor and Chair, member of HAS, M.Sc. in Architectural Engineering
Fields of interest: Large deflections of elastic structures, structural stability and global search of equilibrium, non-linear computation of cyclic symmetric structures, chaotic phenomena in time and space, especially the chaotic states of elastic structures, digital modeling of chaotic motions, connections between discrete and continuous systems, mechanical applications of group theory, parallel algorithms for engineering structures.
Publications: 1 book, 6 chapters in a book, 63 refereed papers, 302 presentations
Fellowships: Member of several doctoral committees, Chairman of the Doctoral Committee of the Faculty of Architecture, BME (2000-), Leader of the Pál Csonka Doctoral School, Secretary of the Mechanical Committee of the HAS (1996-1998).

Although BVM Épelem Ltd. is not a member of the RET consortium, it is expected to be one of the industrial users of the research results. BVM Épelem Ltd. is one of the main companies in Hungarian pre-cast reinforced concrete industry. It produces large amounts of pre-stressed beams for building and infrastructural construction. Initial spatial deformations (lateral displacement and torsion) of pre-stressed bridge beams over a span of more than 30 m often makes their erection impossible. There are currently no reliable methods capable of predicting such unfavorable deformations. The proposed algorithm enables users to calculate spatial deformations in the design phase. BVM Épelem Ltd., as an external contributor, takes part in the research activities through professional consulting activities. It shares its experience and carries out comparative experiments on beams.

Antal Tápai graduated as a civil engineer from the Technical University of Budapest in 1964. He is an expert engineer of structural engineering (1979). He started his career at the legal predecessor of BVM Épelem Ltd. Since the company's privatization, he has been its technical head manager. He took part in important developments including the reconstruction of BVM Épelem Ltd's factory. He worked on the product development of wall elements for the Budapest, Praque and Calcutta metros – a contribution as a result of which he has achieved an international reputation. He also took part in the structural development of several architectural investments (Budapest Sports Hall, schools). He played an important role in establishing the production of pre-cast tramline elements and bridge beams. He taught at the Ybl Miklós College for 20 years. Since 1993, he has been the leader of the pre-cast group of ÉTE (Association on Building Science). He is also member of the Hungarian Group of fib. (Fédération Internationale du Béton). He is Chairman of the Hungarian Concrete Association.

Objectives

The Parallel Hybrid Algorithm developed at the BME solves boundary value problems in a different way than traditional solutions. The result of this is a system which delivers more precise and global solutions at the price of being calculation resource intensive. The algorithm was already used in many engineering and research problems. Our aim is to create an easily configurable and widely available system. The service developed in the scope of this project is planned for sizing pre-stressed bridge beams. The project captures activities ranging from algorithm development to service start up.

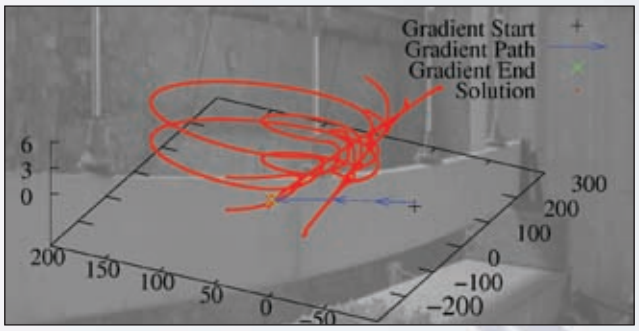
The basic aim at the beginning of the project was to create an algorithm that reliably models the deformation of the pre-stressed bridge beams. It was followed by the application of the algorithm into Grid infrastructure and the development of a graphical interface for the service.

Summary of the activities in previous work stages

We developed an algorithm, reliable in both numerical and physical ways, capable of calculating the cracking of asymmetric concrete beams. The algorithm was then implemented into the Parallel Hybrid Algorithm developed earlier on at the Department of Mechanics, Materials and Structures of BME. Due to the high calculation needs, the algorithm was run in a Grid environment for which we used the infrastructure of MEGA and EGEE.

In parallel with the above changes we created a user interface portal which allows for non-IT users to run calculations with different parameters and display their results on graphical interface.

Besides the above achievements we developed a Gradient Hybrid Algorithm (GHA) to speed up the previous method. Its essence lies in the creation of a special landscape the minimum of which coincides with the solutions of the original problem. The proof of concept implementation of the GHA was finished in the second stage of the project, with the use of the GNU Scientific Library for the gradient algorithm. The method proved to be reliable and fast but it was discovered that its different nature made it impossible to integrate it into the framework of the PHA. The result of it was the creation of a new code based for the functions of the PHA which was completed



in the third phase. The new code is capable of providing the advantages of both the new and the old algorithm, in other words it is capable of doing a combination of the full parameter sweep, path following hybrid and the gradient method. We also changed the parallel nature of the code which was Master-Slave in the PHA and became parameter study (with little overlap) in the new one. This made the usage of Grid infrastructure much easier.
We also performed sample calculations for real-life problems of pre-fabricated concrete beams for some contractor companies. For example, we calculated second order stress of spin technology pillars for ASA Ltd. These companies are usually only able to calculate planar effects. For them, accurate spatial calculations can be an important competitive edge. So we had fabricated 6 asymmetrically pre-stressed beams and measured the structural changes under stress. We compared these results to the prediction of the algorithm. We carried out the experiments with the help of BVM Épelem Ltd. We designed the specimens in a way that allowed not only for the measurement of initial deflections after pre-stressing, but also for the measurement of deformations caused by the loading of the beams, and thus the cracked phase could be compared to numerical predictions. We used the hydraulic loading machine of BVM Épelem Ltd., and used mechanical clocks to measure the vertical and horizontal deflections of the beams. The developed algorithm predicts the vertical and lateral deflections of the cracked beam with a 10% error at the very worst, which is considered highly accurate in industrial applications.

Summary of the activities in the third work stages

The most important work of the third stage was the further development of the GHA algorithm. With the help of the new gradient algorithm, the exponential computation need of the problem was reduced to polynomial times, which allowed the simulation of more complicated problems, like spatial behavior of framed systems. Furthermore, we changed the parallelization nature of the code to fit better the requirements of Grid infrastructure, which widens its usability. The motivation of this work was the already mentioned demand from the concrete industry to calculate deformations of framed systems.

The results and products of the project

- We developed an algorithm capable of modeling the deformation and cracking of pre-stressed concrete bridge beams creditably both numerically and physically.
- The cracking algorithm was implemented into the PHA framework
- We developed the data-structure for the user interface portal
- We developed the GHA algorithm
- We developed the independently parallelizable version of the code which can now be run on any Grid infrastructure
- Based on the results of the algorithm we had fabricated 6 asymmetrically pre-stressed beams and measured the structural changes under stress, which confirmed the numerical results
- All of our results were also used in the university education

4.3 IT security laboratory (subtask 2.2)

Grid an IT security laboratory direction

Project manager: Szabolcs Szigeti

Objectives

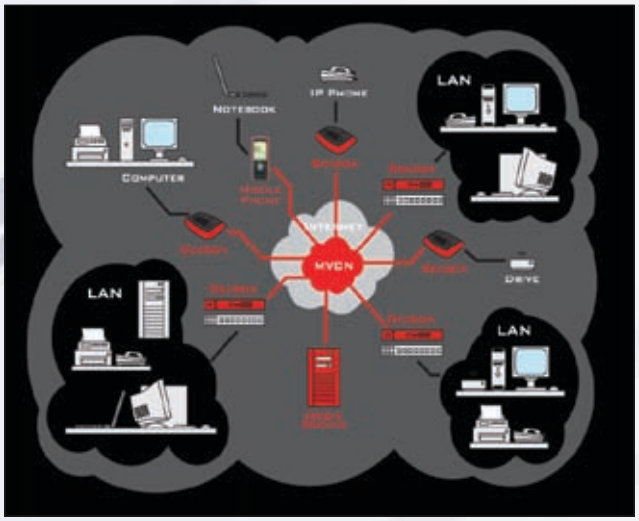
Measuring the security of IT systems poses a great challenge to developers and users. The ISO15408 standard, known as Common Criteria (CC), facilitates security assessment. CC certifications are accepted in Hungary, but there is no accredited laboratory that is able to perform such evaluation and certification. The primary objective of the project is to gain the specialist knowledge and create the methodologies required to initiate the creation of such a laboratory. The laboratory will be able to perform CC evaluations and offer other IT security related services.

Summary of the activities in previous work stages

During the first stage, the physical structure of the laboratory was implemented. This includes the laboratory site and the information technology infrastructure. The members of the project created the procedures and methods for CC evaluation, and a pilot evaluation project was initiated to evaluate secbox, a product of one of the industrial partners of the Knowledge Centre. At the same time, the Melasz Ready programme for the certification of electronic signature products was continued, and the laboratory is now ready to offer this as a service.

The main objective of the second stage is to finish two ongoing CC evaluation projects. The products of two industrial partners of $(IT)^2$ were evaluated. One is secbox, which was started in the first stage, and the other is Zorp firewall, whose evaluation was started in the second stage. A further goal was to provide IT security services, in particular vulnerability evaluation. In order to achieve this, an Ethical Hacking methodology and service was developed.

The $(IT)^2$ project for the development of secbox used the services of the security laboratory to prepare the product



for CC certification. An important milestone was reached when one of the most important documents, the Security Target (ST) was created. It was accepted by the German institute performing the certification. Other important documents were also compiled. Zorp evaluation is a separate $(IT)^2$ project.

As a separate activity of the second stage, a methodology for Ethical Hacking was developed. The need for this service was discovered on market analysis and discussions with various industrial partners during the first stage. Ethical Hacking is an evaluation method that uses

“hacker” tools and procedures to practically evaluate vulnerabilities of a system or organisation. Our methodology combines Ethical Hacking with other, formal evaluation and certification standards (such as ISO27001, Cobit, CC and ITIL). On the basis of this methodology, we have created a complete service, which includes the knowledge base, its supporting tool and marketing. We introduced our service at the ITBN 2007 (Day of IT Security) conference.

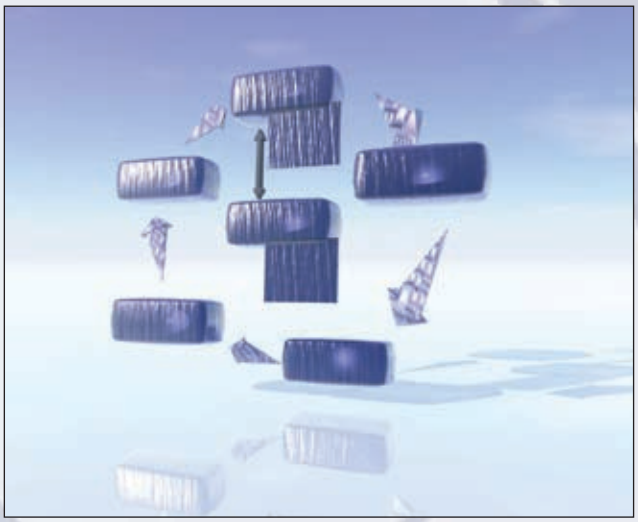
Summary of the activities in the third work stages

The main objective of the third stage was the operation of the laboratory. We concentrated on providing Ethical Hacking services.

The secbox evaluation was also continued, as the new version of the firmware was analyzed using Ethical hacking methods.

Providing Ethical Hacking services was also an important task. We have enhanced our service, with continuous internal trainings and refinements to our methodology. Marketing for Ethical Hacking was started at the end of the second stage. As a result, a web site (http://ethack.it2.bme.hu/) has been set up, where information materials were published. We have also used direct marketing to reach potential customers.

As a result, we have received several requests for Ethical Hacking. At the beginning of this stage, a multinational transport engineering company asked for security evaluation of their IT infrastructure. The proposal we laid down in response was accepted. We began our work by drawing up a detailed plan. During the Ethical Hacking, we tried to penetrate the network of the customer, finding holes which might lead to compromise of the security. At the end of the test, we presented the findings to the customer. They indicated that they were satisfied with the work of the laboratory, and planned to use its services in the future.



The laboratory has received other requests, our offers are currently being prepared. We are ready to provide services in CC preparation and Ethical Hacking, and are working on developing new IT security services.

The results and products of the project

- IT security laboratory (infrastructure).
- secbox CC evaluation preparation (documentation).
- Ethical Hacking methodology (documentation).
- Ethical Hacking support tools (software).
- Ethical hacking service (service).
- Ethical hacking marketing material (web site, documentation).

PUBLICATIONS

The research publications put out by the BME (IT)² Knowledge Centre over the past few years have been compiled. Actual activities were performed within four R&D programmes and their results were made use of in four application-development directions. The list of publications is given here categorised within the four application-development directions:

e-Document direction

Juan de Lara, Tihamer Levendovszky, Pieter J. Mosterman, Hans Vangheluwe: Second International Workshop on Multi-Paradigm Modeling: Concepts and Tools, MoDELS Workshops 2007: LNCS 5002, pp.: 237-246, Springer.

Bogárdi-Mészöly Ágnes, Levendovszky Tihamér, Charaf Hassan és Szeghegyi Ágnes: Effect Analysis of an Improved Performance Evaluation Algorithm, 6th International Symposium on Applied Machine Intelligence and Informatics (SAMI 2008), Slovakia, Herl'any, 2008. január 21-22., IEEE Catalog Number CFP0808E-CDR, ISBN 978-1-4244-2106-0, 125-130.o.

Bence Kovari, Gergely Kiss, and Istvan Albert: Stroke Matching for Off-line Signature Verification based on Bounding Rectangles, IEEE ISCIS 2008, 23rd International Symposium on Computer and Information Sciences 2008

Bence Kővári, Gergely Kiss, Hassan Charaf: Stroke Extraction and Stroke Sequence Estimation for Off-line Signature Verification, The Eighth IASTED International Conference on Visualization, Imaging, and Image Processing, Palma de Mallorca, Spain 2008

Bence Kővári, István Albert, Hassan Charaf: A General Representation for Modeling and Benchmarking Off-line Signature Verifiers, 12th WSEAS Int. Conf. on COMPUTERS, Heraklion, Grecce 2008

Middleware, Knowledgebase and Graphical application direction

Umenhoffer Tamás, Szirmay-Kalos László, Szécsi László, Tóth Balázs, Mateu Sbert: Partial Multi-Scale Precomputed Radiance Transfer; In: Spring Conference on Computer Graphics. Budmerice, Slovakia, 2008.04.21-2008.04.23. 2008. pp. 87-94.

Umenhoffer Tamás, Szirmay-Kalos László: Interactive Distributed Fluid Simulation on the GPU; In: Petar Biljanovic, Karolj Skala (szerk.); MIPRO 2008: Grid and Visualization Systems. Opatija, Croatia, 2008.05.26-2008.05.30. pp. 236-242.

Tóth Balázs, Szirmay-Kalos László: Deferred shading in distributed visualization; In: Petar Biljanovic, Karolj Skala (szerk.); MIPRO 2008: Grid and Visualization Systems. Opatija, Croatia, 2008.05.26-2008.05.30. pp. 295-300.

Tamás Umenhoffer, Gustavo Patow, László Szirmay-Kalos: Caustic Triangles on the GPU ;In: Tolga Capin, Tat-Seng Chua, Daniel Thalmann (szerk.); Proceedings of Computer Graphics International: CGI. Istanbul, Turkey, 2008.06.09-2008.06.11. pp. 222-228.

Szirmay-Kalos László: Monte-Carlo Methods in Global Illumination; Saarbrücken: 2008. 128 p.VDM Verlag Dr. Müller Aktiengesellschaft & Co.

Szirmay-Kalos László, Szécsi László, Mateu Sbert: GPU-based Techniques for Global Illumination Effects; Morgan and Claypool Publishers, 2008. 270 p.

Szécsi László, Szirmay-Kalos László, Mateu Sbert: Interactive Global Illumination with Precomputed Radiance Maps; In: Wolfgang Engel (szerk.); „ShaderX 6": Advanced Rendering.; Charles River Media, 2008. pp. 401-410.

László Szirmay-Kalos, Tamás Umenhoffer; Displacement Mapping on the GPU - State of the Art; COMPUTER GRAPHICS FORUM 27:(1) 1-21 (2008) IF: 1.164

Antal György, Szirmay-Kalos László: Fast Evaluation of Subdivision Surfaces on Direct3D10 Graphics Hardware; In: Wolfgang Engel (szerk.); „ShaderX 6" Charles River Media, 2008. pp. 5-16.

Balázs Csébfalvi: An Evaluation of Prefiltered Reconstruction Schemes for Volume Rendering; IEEE TRANSACTIONS ON VISUALIZATION AND COMPUTER GRAPHICS 14:(2) 289-301 (2008) IF: 1.794

Balázs Csébfalvi: BCC-Splines: Generalization of B-Splines for the Body-Centered Cubic Lattice; JOURNAL OF WINTER SCHOOL OF COMPUTER GRAPHICS 16:(1-3) 81-88 (2008)

Szirmay-Kalos László: Simulation and Rendering of Fluids on a GPU Cluster. HP Advanced Visualization CCN. Teleconference, March 6, 2008. http://amon.ik.bme.hu/hpccn/

Balázs Domonkos, Kristóf Ralovich: Parallel Visualization of the Sloan Digital Sky Survey DR6. Journal of WSCG, Vol.16, No.1-3, ISSN 1213-6972, ISBN 978-80-86943-14-5, 2008.

Liktor Gábor: Ray tracing implicit surfaces on the GPU, CESCG Conference, Budmerice, 2008.

Klár Gergely: Flow Simulation using Obstacle Dependent Grids. CESCG Conference, Budmerice, 2008.

Klár Gergely: Level of Detail Flow Simulation, Eurographics Conference, Short papers, Cyprus, 2008.

Illés Dávid, Horváth Péter: SPH-based Fluid Simulation in Distributed Environment. MIPRO International Convention on Grid and Visualization Systems conference, Opatija, Croatia, 2008.

Simon B., Dr. László Z., Dr. Goldschmidt B.: SOA mintarendszer kialakításának tapasztalatai, Networkshop 2008, Dunaújváros, 2008. március 17-19.

B. Simon, Z. László, B. Goldschmidt: SOA Interoperability, a Case Study, Proceedings of the IADIS International Conference, Informatics 2008, Amsterdam, The Neatherlands, July 25-28, 2008. pp. 131-138.

e-Security development direction

Bóka G.: Szoftvertermék-jellemzők mérése teszteléssel, Szoftvertesztelés Workshop az IIR (Institute for International Research) szervezésében., Budapest, 2008.06.05

Z. D. Kelemen, K. Balla, J. Trienekens, R. Kusters: Towards supporting simultaneous use of process-based quality approaches, in: Proceedings of 9th International Carpathian Control Conference: ICCC´2008. Sinaia, Romania, 2008.05.24-2008.05.28., 2008. pp. 291-294.

Kelemen Z. D., Balla K.: A CMMI-DEV v1.2 és az ISO 9001:2000 kapcsolata, Magyar Minőség 17:(2) 27-40 (2008)

Z. D. Kelemen, K. Balla, G. Bóka, Support for synergic use of multiple quality models, SEPG Europe 2008, Munich

K. Balla: Synergic Use of Software Quality Models, In: Ravi Kumar Jain B (ed.) Software Quality Measurement: Concepts and Approaches., Icfai University Press, 2008. pp. 154-173.

Balla K.: A SOX törvény alapjai és informatikai vonatkozásai, CIO 08 – Hangszerelés változásszimfóniára - Informatikai döntéshozók konferenciája Siófok, 2008 április 17-18

B. Goldschmidt, G. Gyánó, Z. László: Java-C++ bridge for Symbian based smartphones, in Proceedings of the ICETE International Joint Conference on e-Business and Telecommunications, July, 2008, Porto, Portugal, pp. 241-244.

Soóki P., Zelenák J.: MVCN – menedzselhető virtuálisan zárt hálózat, IP-alapú hálózatok biztonsága – új technológiák szakmai workshop, 2008. július 31., Budapest.

Zelenák J., Kuti G.: Navayo secbox – Building private closed secure virtual network CeBIT Hannover, 2008. március 4-9.

Kuti G.: Navayo secbox – Building private closed secure virtual network IT ChannelVision, 2008. május 20-23. (Texas, USA)

Kuti G., Soóki P.: Navayo secbox – Building private closed secure virtual network Tokió, Japan, 2008. május 26.

Grid and IT Security laboratory direction

J. Török, D. Kadau, L. Brendel, D. E. Wolf, Shear band patterns in biaxially sheared granular media, Physical Review E, (in the press).

Péter Dóbé, Richárd Kápolnai and Imre Szeberényi: Saleve: toolkit for developing parallel Grid applications, Híradástechnika, vol., LXIII, 2008. pp., 60-64.

Pasztuhov Dániel, Sipos András Árpád: Grid alkalmazása peremérték feladat megoldására, GRID délután, BME IK, 2008.02.13.

Szeberényi Imre: GRID mint közmű – a technológia fejlődése, változása, GRID délután, BME IK, 2008.02.13.

Andras Arpad Sipos (BME), Gert van der Heijden: A global numerical method for finding isolated solution branches with applications to a conducting elastic rod in a uniform magnetic field, workshop on Bifurcations in Dynamical Systems with Applications, Department of Mathematics, Bielefeld University, 2008.05.19-22.

Dénes Németh: Synchronizing Multiple Lustre File Systems, HP Consortium for Advanced Scientific and Technical Computing users group meeting, 2007.11.9-10

Máté Lakat, Dénes Németh, János Török and Imre Szeberenyi: gLite WN running as a Windows Service, EGEE08, Istanbul, 2008.09.21-26.

Kiállító stand az EGEE07 konferencián, Budapest 2007. 10.1-5

Kiállító stand az SC EGEE07 konferencián, Reno, USA, 2007.11.9-16

Szigeti Szabolcs , Pánczél Zoltán, ,Szabó Péter: Jobb ha mi törjük fel - ethical hacking a gyakorlatban Networkshop 2008, Dunaújváros, 2008. március 17-19

Szigeti Szabolcs, Szeberényi Imre: IT biztonság az e-közigazgatásban - az e-közigazgatási keretrendszer projekt ITBN 2008, Budapest, 2008. szeptember 25.

MARKETING COMMUNICATION OF THE KNOWLEDGE CENTRE

The Knowledge Centre strived to enhance the existing cooperation between university research laboratories and the industry, and endeavoured to boost its efficiency. Its aim was to create marketable products and services and to see to their exploitation in the economy.

On the one hand, the communication of BME (IT)^2 promoted its efficient operation. On the other hand, by presenting the competencies and results of the Knowledge Centre, it created a positive image and a supporting environment that brings the Knowledge Centre to the forefront when innovation or R&D needs arise in the industry, or when their implementation is contemplated.

Associates of the Knowledge Centre worked to inform the industry and the public about our objectives, actual professional activity and our results by way of events organised by the Knowledge Centre, at conferences, exhibitions and workshops in Hungary and abroad, as well as by means of direct marketing. The communication was supported by unified image and communication tools (flyers, brochures, posters, placards).

Major events:

Professional introduction
Professional introduction representing the R&D and innovation cooperation between the IT industry and BME. Those interested could view an on-line broadcast of the event on the Internet. (29 March, 2006)

European Research and Innovation Exposition
At the Hungarian research, innovation and technology stand, six Hungarian research institutes were represented through the organisational and financial support of NKTH , among them BME (IT)^2 (Paris, 8-11 July 2006).

IT Security Day
The largest event dealing with IT security in Hungary, organised by ITBN. The most significant developer, consulting and commercial companies of Hungary participated in the event. Knowledge Centre associates are constant participants of the all-day conference and related exhibition, organised annually under the auspices of BME (IT)^2 (September 2006/2007/2008).

CeBIT 2007
The CeBIT Information and Communications Technology trade and fair is an excellent opportunity to get to know the global market trends, to form new connections and introduce our results. BME (IT)^2 represented itself with its own exhibition booth in the 'Future parc' exposition area. For the week of the fair the ICT industry of the world was concentrated in Hannover, thus attendance helped the

joint innovation achievements of the Knowledge Centre partners to gain great publicity (Hannover, 15 - 21 March, 2007).

European Institute of Innovation and Technology, expert's hearing.
Dr. Péter Risztics, director, was invited to deliver a lecture before the Council of the European Union at the expert's hearing of the workgroup on preparing the EIT and Knowledge Innovation Centres. (Brussels, 5 March, 2007)

EGEE'07
The largest European Grid event in 2007, the EGEE '07 conference was jointly organised by BME (IT)^2 and the BME Centre for Information Technology. The conference broke several records as to the number of lectures and participants. The number of participants surpassed 600, representing 47 countries from all walks of life, including public administration, finances and business. The conference was home to 275 lectures in 86 sections in 5 days (Budapest, 1-5 October, 2007).

Supercomputing exhibition and conference (SC '07)
The world's largest supercomputing exhibition and the related conference is organised annually in November in the United States of America. At the 2007 conference in Reno, Nevada, the Parallel Compositing Library, a product of the cooperation between HP and BME (IT)^2 won the editor's and reader's award for the category visualisation technologies of the magazine HPCwire, a leading

journal in the field of high-performance computing. The library was developed and tested on HP's class C blade systems. The award acknowledges the joint achievement of HP and BME (IT)². At the SC '08 in Austin, Texas, BME (IT)², as a member of the Hungarian Grid Competence Centre, exhibited once again in the field of distributed and extended file systems

Innovation Forum

The Embassy of the Republic in Hungary in Berlin, in close collaboration with the Ministry for Economy and Transport, organised a conference on innovation in the newly inaugurated building of the Hungarian Cultural Centre, Collegium Hungaricum. At the conference, Knowledge Centre associates delivered lectures on the cooperation between university and industry, and the results it had given rise to. Besides presenting the innovation development results in Hungary, the event also aimed at extending the R&D network of Hungarian innovation centres, promoting new partnership cooperations and fostering the marketing of our results, products and novel solutions on the German market (Berlin, 21 April, 2008).

Europe Innova – „User-driven innovation tour"

On their innovation tour, the participants of EUROPE INNOVA partner meeting and conference could visit the R&D&I workshops of the BME (IT)², where short demonstrations were held on the development projects of the Knowledge Centre (Budapest, 2 June, 2008).

The following table gives a summary of our major media exposure:

Medium	Date	Title	Genre
IT-BUSINESS TODAY	2006. március 28.	Holnap Történik	Article
HWSW	2006. március 30.	Innovációs és tudásközpontot adott át BME-n..	Article
IT-BUSINESS TODAY	2006. március 31.	Hazai Hírek	Article
IT.news	2006.március 31.	IT-tudásközpontot avattak a Műegyetemen	Article
Index	2006. március 31.	Tudásközpont nyílt meg a BME-n	Article
Élet és Tudomány	2006. április 13.	Átadták az IT Innovációs és Tudásközpontot	Article
Világgazdaság	2006. május 9.	Egyterű k+f+i műhely megnyitása	Article
ECHO TV	2006. május 9.	Tabuk nélkül	Interview
Echotv.hu	2006. május 10.	Innovációs műhely a BMGE-n	Article
Prím Online	2006. május 10.	Újabb tudásközpont a Műegyetemen	Article
Magyar Hírlap	2006. május 10	Innovációs műhely a BMGE-n	Article
Metro	2006. május 11.	Közös ipari-egyetemi fejlesztési műhely	Article
MTI	2006. május 15.	Átadták a műegyetem K+F és innovációs műhelyét	Article
Világgazdaság	2006. május 19.	K+F+I: egy ernyő alá terelik az innovációt	Article
DUNA-TV	2006. július 10.	HEURÉKA megtaláltam	Interview
MISKOLCI TV	2006 szeptember	Klick, innovációs magazin	Interview
euroAstra.hu	2007. március 20.	Ismét CeBIT-en..	article
Iseesec.hu	2007. március 20.	CeBIT 2007	article
PrimOnline.hu	2007. március 20.	Ismét a CeBIT-en	article
IT-business	2007. szeptember 18.	IT Security Special	interview
Index.hu	2007. szeptember 24.	Hacktivity 2007 Owned	article
Compterword	2007. szeptember 25.	ITBN 2007	news
Hup.hu	2007. szeptember 26.	A hét képe	forum
Mta.hu	2007. szeptember 26.	Világ számítógépei, egyesüljetek!	news
IT.news.hu	2007. szeptember 30.	GRID-csúcs Budapesten az EGEE jegyében	article
aHirek.hu	2007. szeptember 30.	GRID-csúcs Budapesten.	news
Eu-ecss.eu	2007. szeptember 30.	EGEE'07Conference	news
PrimOnline.hu	2007. október 1.	Hatszázan az év legnagyobb európai Grid rendezvényén	article
HírTv	2007. október 1.	EGEE 07 Konferencia a Műegyetemen	article
IT-business.hu	2007. október. 1.	EGEE'07 Konferencia	news
GRIDtoday	2007. október 1.	Breaking New: EGEE'07	article
Hiradó.hu	2007. október 2.	Az év legnagyobb európai Grid-rendezvénye Bp-en	article
Infovilág	2007. november 22.	A világ legjobbjai között a BME és a HP közös kutatása	article
Observer	2007. november 23.	A BME és HP együttműködésében fejlesztett…	article
Computerworld	2007. november 26.	A világ legjobbjai között a BME és a HP közös projektje	article
Számítástechnika	2008. február 12.	Biztonságos betörő	article
NOL	2008. június 2.	Tokióban hódít a magyar informatika	article
Népszabadság	2008. június 3.	Távol-Keleten hódít a magyar IT-biztonsági cég	article
IT-business	2008. szeptember 16.	IT Security Special	article

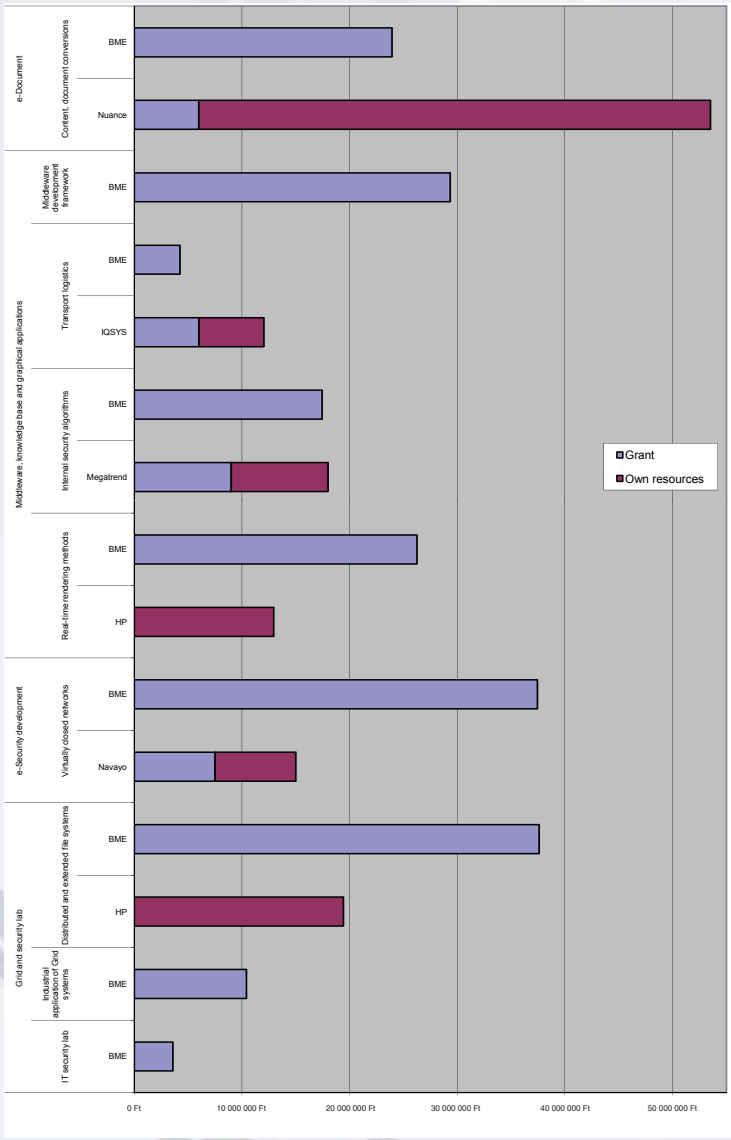
INDICATORS

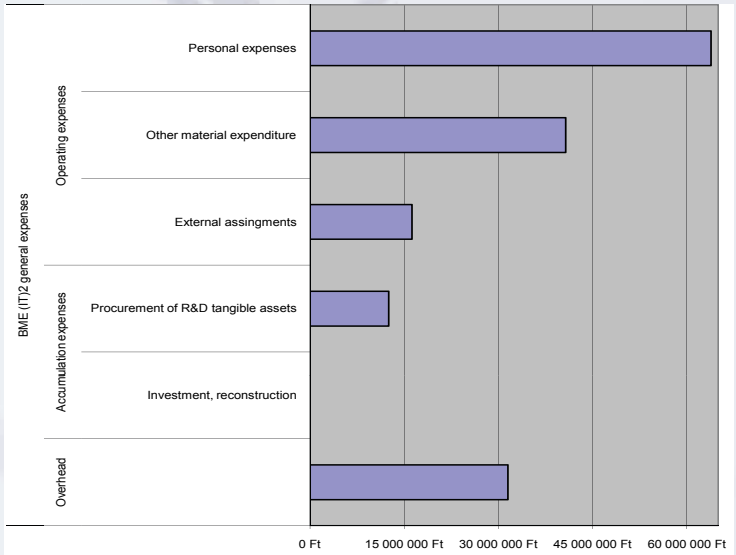
Indicators of accomplishments in BME information Technology and Knowledge Centre

1	Exploitable achievements of the project		Year 2008 plan	Year 2008 fact	Consolidated plan	Consolidated fact
	New developments	product	1	2	11	12
		service	2	2	11	11
		technology	2	3	11	13
		application	6	6	13	19
		prototype	5	5	17	21
	Benyújtott szabadalmak száma	domestic	1	0	1	1
		PCT	1	0	1	0
		foreign	2	0	2	1
	Industrial property, trademark, know-how		3	3	4	5
2	Scientific results		Year 2008 plan	Year 2008 fact	Consolidated plan	Consolidated fact
	Publications (conferences included)	domestic	14	11	39	51
		international	11	35	26	78
	Dissertations	PhD	4	4	5	5
		DHAS	0	0	0	0
	Hav they resulted in new international projects? (Y/N)		Y	Y	Y	Y
3	Human resource		Year 2008 plan	Year 2008 fact	Consolidated plan	Consolidated fact
	Are projects used in education? (Y/N)		Y	Y	Y	Y
	Involved in the projects	number of university	20	23	53	82
		number of PhD students	15	10	41	40
		number of young researchers	5	16	16	38
	Researchers granted scientific degree		2	1	3	2
	Number of people employed as result of the project	at enterprises	12	20	33	47
		at researchers institute	36	24	107	116
		total number of resarchers	29	16	86	93
4	Economic use		Year 2008 plan	Year 2008 fact	Consolidated plan	Consolidated fact
	Institutions taking part in the activities of the Knowledge Centre	number of research institutes	8	8	17	17
		number of enterprises	15	16	31	36
	Number of new enterprises founded as result of the project		2	1	4	2
	Revenue of the new enterprises		58630	0	70000	0
	Have the project results been put to economic use?(Y/N)		Y	Y	Y	Y
	Number of enterprises utilising results from the project		8	8	20	22
	Income arriving from the project	surplus revenue (eFt)	801 340	1 028 200	1 374 000	1 413 823
		export revenue (eFt)	649 450	955 000	1 135 000	1 229 159
		expense decrease (eFt)	470 000	128 700	740 000	128 700
5	Social use		Year 2008 plan	Year 2008 fact	Consolidated plan	Consolidated fact
	Are the project results presented in public?		Y	Y	Y	Y
	Type of presentation	in professional scope	Y	Y	Y	Y
		in public scope	Y	Y	Y	Y
6	Other, special monitoring indicators derived from this project		Year 2008 plan	Year 2008 fact	Consolidated plan	Consolidated fact
	Number of courses enhanced with research results from projects		9	6	21	26
	Number of students involved		950	415	2270	3220
	Number of diploma theses prepared from topics in the project		17	21	39	38

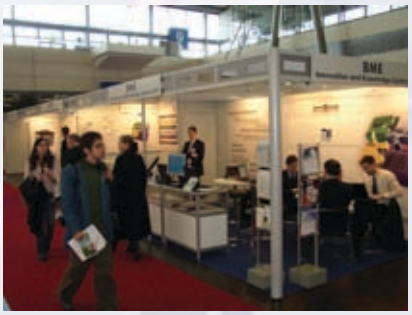
FINANCING

The management policies of BME (IT)^2 Knowledge Centre were established in compliance with the public finance law, higher education law, and the management regulations of NKTH and BME. Specific financial, documenting and accounting processes are carried out with the support of the unified management system (EGR) of BME, under complete transparency and documentation. The Knowledge Centre accepts its income under its own central project code. The financing of all subprojects (in this case totally 14 professional – 9 in 2008 - and 1 innovation and management subproject) will be done from this central project code. Several units of the institution can participate in the realisation of each of the 14 subprojects. Therefore, within the management regulations of the project, the leader of each institutional unit has the disposal of the source under the subcode corresponding to the subproject, according to the agreement with the Knowledge Centre. Based on the progression of the project and the accomplishment of tasks, the Knowledge Centre allows the use of resources under the subproject code in quarterly intervals. The projects carry out wages management under each subproject code (only private expenditures are allowed). Procurements, investments, extermal commisions, management, innovation, PR and communications, along with personal and material expenses linked with other relevant activities (conferences, organised programmes,membership fees,overhead,etc.) are provided from the central project code. The personnel side of the central account is debited to cover all daily allowances of assignments abroad and every supplementary cost incurred. Professionally outstanding performance of projects is also rewarded using this account. With the help of the established method, the Knowledge Centre management processes can run together and in a clear, auditable way even at the level of projects. The member institutions of the industrial consortium cooperating in the Knowledge Centre also conduct their management processes in compliance with legal and application constraints. Their financial and accounting processes linked with the RET-project will be viewed by professional auditors in quarterly intervals. For the sake of clarity, the financial data of the Knowledge Centre in 2008 of operation, can be summarised in the following diagram:





ABBREVIATIONS



BME:
Budapest University of Technology and Economics

(IT)²:
Information Technology Centre for Innovation and Knowledge

AAIT:
Department of Automation and Applied Informatics

AJAX:
Asynchronous JavaScript and XML

BKSz:
Budapest Transport Association

CC:
Common Criteria

CISA:
Certified Information Systems Auditor

CISSP:
Certified Information Systems Security Professional

CMM:
Capability Maturity Model

CMMI:
Capability Maturity Model Integration

COBIT:
Control Objectives for Information and related Technology

DPM:
Dynamic Programming Method

EGEE:
Enabling Grids for E-scienc

E EXT:
Enterprise Express Text

FIB:
Federation Internationale du Beton

FME:
Feature Manipulation Engine

GIS:
Geographic Information System

GQM:
Goal-Question-Metric

ECOP:
Economic Competitiveness Operational Programme

HMM:
Hidden Markov Model

IIT:
Department of Control Engineering and Information Technology

IK:
Centre of Information Technology

IPS:
Intrusion Prevention System

ISO:
International Organisation for Standardisation

IST:
Information Society Technologies

M(LD)M:
MultiLayered and -Dimensional Metamodel

MDA:
Model Driven Architecture

MIBÉTS:
Hungarian Scheme of Information Security Assessment

MGKK:
Hungarian Grid Competence Center

MOF:
Meta Object Facility

MVCN:
Manageable Virtual Closed Network

NAT:
National Board of Accreditation

NAVA:
National Audiovisual Archive

NIIFI:
National Institute of Information Infrastructure Development

PHA:
Parallel Hybrid Algorithm

PRINCE:
Project Run in Controlled Environment
SCAMPI Standard CMMI Assessment Method for Process Improvement

SDX:
Signed Document eXpert

SFS:
Scalable File Share

SOA:
Service Oriented Architecture

SOAP:
Simple Object Access Protocol

SPC:
Statistical process control

SPICE:
Software Process Improvement and Capability dEtermination

SSADM:
Structured Systems Analysis and Design Methodology

ST:
Security Target

SVA:
Scalable Visualisation Array

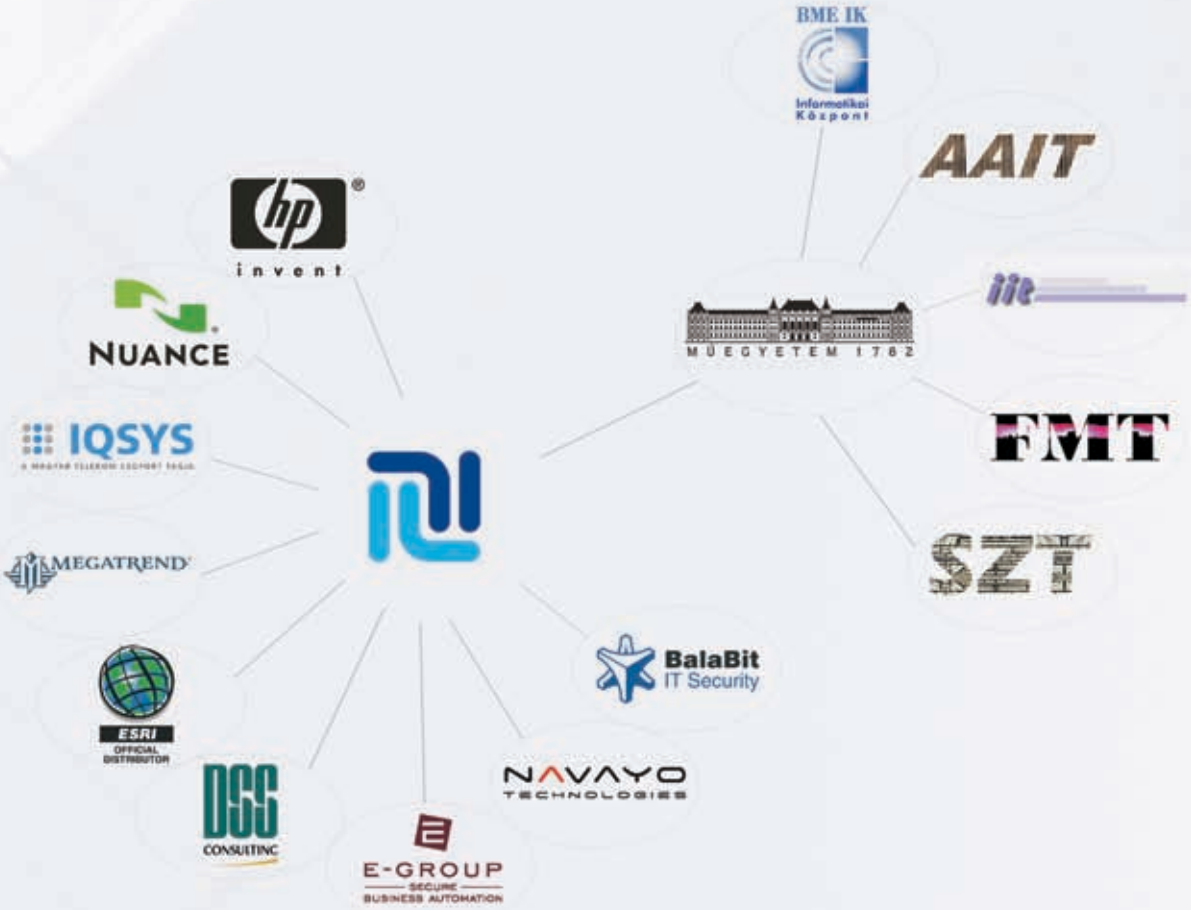
SVC:
Signature Verification Competition

SzT:
Department of Mechanics, Materials and Structures

TÉT:
Scientific and Technological Co-operation

VoIP:
Voice over Internet Protokoll

XML:
eXtensibel Markup Language



The publication was prepared within the framework of Pázmány Péter Programme, with the support of NKTH.

Published by the BME Innovation and Knowledge Centre of Information Technology

H-1117 Budapest, Magyar tudósok körútja 2. • Phone: +36-1-463-1188, +36-1-463-1210 • Fax: +36-1-463-1387

www.it2.bme.hu • info@it2.bme.hu

Responsible for publishing: Dr. Péter Károly Risztics