

Higher Education Quality Assessment Center of Estonia

Joint Final Report

# Cybernetica Ltd

Research fields Assessed

Cryptography and Data Security  
Expert Systems Technology  
Balancing Dynamics

Visit Dates

27-29 April 2000

Expert Team

Prof. Dr. Manfred Thoma  
(Team Chairperson)  
Institut für Regelungstechnik  
Hannover University  
Appelstr.11, D-30167 Hannover  
thoma@irt.uni-hannover.de

Kaisa Nyberg, PhD.  
Nokia Research Center  
P.O. Box 407  
FIN-00045 Nokia Group, Finland  
Kaisa.Nyberg@nokia.com

Prof. Dr. Janis Brazdins  
The University of Latvia  
Institute of Mathematics and Computer Science  
Rainis boul. 29, Riga, LV-1459, Latvia  
jbarzdin@cclu.lv

Prof. Dr. Peeter Normak  
Tallinn Pedagogical University  
Department of Mathematics and Informatics  
Narva mnt. 25, 10120 Tallinn, Estonia  
pnormak@tpu.ee

## Part I

# General Overview

The Higher Education Quality Assessment Center of Estonia has invited four experts from Germany, Finland, Latvia and Estonia to review and make accreditation recommendations for three research fields at Cybernetica Ltd (hereinafter called "Cybernetica" or "Company"). The research fields are: 1) Cryptography and Data Security ("CDS"), 2) Expert Systems Technology ("EST") and 3) Balancing Technology ("BT").

The expert team ("Team") visited Cybernetica 27-29 April 2000, according to the prepared Agenda.

The Team was given the following materials:

- Self-Assessment Report (14 pages)
- Annual Report for 1998 (19 pages)
- Strategic Development Plan (in Estonian, 34 pages)
- Additional materials (budget breakdown, presentations slides etc)

The Team discussed presentations given by the following members:

- Dr. Ülo Jaaksoo, The Chairman of Management Board of Cybernetica, gave a general overview about all activities of Cybernetica.
- Prof. Dr. Boris Tamm, the leader of the group Expert Systems and Balancing Dynamics.
- Dr. Monika Oit, the Research&Development director, gave a brief overview of the R&D activities of the company in general.
- Dr. Ahto Buldas, senior researcher at the security systems group.

In order to get a better view of the activities of entire company the Team also visited the Department of Navigation and Surveillance Systems, though the research fields represented there were not subject of the assessment. The Team was given a rather complete overview about the activities of the Department (by Dr. Mart Min and Dr. Harry Tani).

First of all, the Team will point out the following basic facts:

- Cybernetica was established in 1997 by splitting up the Institute of Cybernetics of Academy of Sciences. Being a stock company (owned by the Estonian Republic through Ministry of Education) it has a unique status among Estonian R&D institutions.
- Cybernetica has a very detailed Strategic Development Plan (from June 1998) containing SWOT-analysis for each strategic action line, separately. However, a broader audience will be informed by general Annual Reports.
- The company has three departments (Information Systems, Information Security Systems, Navigation and Surveillance Systems) and employs a little over 100 people with an average age of 36 years. Working conditions are very good (in average about 28 m<sup>2</sup> per person): most of the research staff have personal rooms equipped with modern technology).
- The budget for 2000 is expected to be about 35 MEEK, from which about 35% are spent for personnel costs.

What follows are the detailed description of the working groups (Part II), general recommendations (Part III), accreditation conclusions (Part IV) and accreditation recommendation (Part V).

## Part II

# Research Groups

In this section we characterize every research group separately.

## 1. Cryptography and Data Security

### Presentations, Visits and Discussions

The Team discussed the following presentations of the group members:

- Monika Oit, the director of R&D activities of Cybernetica, listed the main results and achievements of the Information Security Systems Department.
- Ahto Buldas, researcher at the security systems group since 1993, gave a detailed presentation on the current research project *Long-term validation of electronic documents*, where digital time stamping techniques form an essential tool.

The evaluation group did not meet with other members of the department staff. Also the work places of the department remained unvisited due to lack of time. On the other hand, the group was given the possibility to follow online using videoconferencing equipment the research seminar that was going on simultaneously in the Tartu laboratory. The Tartu laboratory belongs to the Information Systems Security Department but it was not visited.

### Activity

The CDS group is working on a relatively new and rapidly growing and developing area of information technology. The group was started as early as 1993 from almost nothing. The first two years was a learning period supported by occasional funding. Today the group has 14 members, has produced both scientific results and successful commercial products. Recently a separate company was founded to do domestic and international marketing and customer support. Hence the information security group offers an example of a new venture that has also become a successful business. More generally, this type of small highly specialized software companies have shown to be potentially successful also elsewhere, and are especially suitable for small countries.

The implementations and products developed by this group are important to the Estonian society also because they have been widely adopted by the national organisations and companies as the principal solution in their information security systems.

The report shows some ad hoc cooperation with Eindhoven University. Otherwise the group has not been very successful in establishing long term partnership with foreign research institutes. The group is encouraged to continue looking for possible cooperation in Europe within the Science for Peace and the European research programmes, for example.

### Research and Development

Development and research of information security techniques is a new and very fast developing area also internationally. The Cybernetica group is not unique, similar work and development is carried out in many institutions around the World. It is also very typical that this area of research and development attracts young people and the atmosphere is enthusiastic and dynamic. Cybernetica has been successfully benefited from the favorable trend around this area of research.

The research and development work done by this group also compares favorably to other similar companies. First, it has a leading edge in research of one of the crucial techniques, digital time stamping, which for a long time was neglected. This group was the first in the world to start developing these techniques. Secondly, the group has used various channels to promote the deployment of information security techniques: international standardization, legislation, and articles and presentations aimed to general audience.

The strategy of research has apparently been successful. A small group must specialize in order to achieve international level. On the other hand, wide coverage of expert knowledge is needed for development of comprehensive information security solutions and products.

The evaluation does not cover the quality of software development processes in use. The use of Rational Unified Process methodology and tools for software development was reported.

### **Publications**

The self-assessment report lists all publications since 1993. There are two books in Estonian about the foundations of information security mainly targeted for security managers of Cybernetica's customer companies. Out of the 20 scientific papers 6 have appeared in international conference proceedings, out of which two are well-established and have rigorous refereeing process. The listed 31 research and project reports are mainly for internal use and education. So far one PhD thesis and one master's thesis have been completed in the area of information security. In addition, the group has been very active in writing and publishing articles for general audience.

### **Competence and Education**



The key personnel of the group consists of two people, who apparently share the duties of the department leadership. The entire department including the Tartu laboratory has 14 members out of which 4 PhD students and 6 MSc students. Out of the 10 students 6 are in Tartu. As a rule the students are full time employed by the company, and their research topics and thesis work is closely connected to the product development work they do for the company.

The competence of the two leading staff members is excellent. They have the proper education, several years personal experience in this area and remarkable devotion and enthusiasm. The other members have proper basic education in order to develop further their research skills in this area.

The group has been very active in giving the basic knowledge in the science of Cryptography and Information security by lecturing on these topics at the national universities and supervising masters and doctors theses in this area. Also the company supports continuous learning process by organising regular research seminars for its employees.

## **2. Expert Systems Technology**

### **Presentations, Visits and Discussions**

Boris Tamm, the leader of the group, gave a detailed presentation on the current research project Expert Systems. Unfortunately, the evaluation team did not have the possibility to meet the main contributor of the project, K. Taveter.

### **Activity**

This is a new direction for Cybernetica, started only a couple years ago. In this moment the research group is very small consisting of only one doctoral student and one master student.

### **Research and Development**

Main objective of the research is how to combine the three most popular techniques of software development: object oriented approach, rule-based approach, and agent techniques. This is one of the most actual topic in software engineering. Results obtained by this group are a good contribution in this area.

### **Publications**

There are at least 5 publications in high level international conference proceedings. It is a good record for such a small group.

### **Competence of the Research Group**

Competence of the research group is high which is confirmed by the publications. There is active international cooperation and the principal contributor K. Taveter is currently working and doing research in Finland at the State Research Centre. The only problem we see here is that the research group is too small for such a wide topic.

The research direction is of large importance for Estonia: object-oriented and agent technologies become basic technologies in software engineering, and more experts are needed in Estonia in this field.

## **3. Balancing Dynamics**

### **Presentations, Visits and Discussions**

The chairman of the evaluation Team had a chance to visit the laboratory already on April 26, a day before the official meeting. Some demonstrations have been prepared. Besides he had an intense discussion with the leader of the group Boris Tamm and the real expert in grinding Aleksei Tümanok, PhD, an experienced lecturer and researcher in the field of Applied Mechanics, holder of several patents, and consulting expert for enterprises. On the next day B. Tamm gave a detailed presentation on the project to the complete Team.

### **Activity**

The work of this research group is mainly focused on applied research and development of automatic balancing of rotating systems with a permanently changing mass. It is a complicated task because one has to deal with hypercritical velocities and large masses which are continuously changing depending on time and space.

The objective of the project is to analyse the dynamics of the rotating system with nonlinear characteristics. In the last two years (1998-1999) four different adaptive regulators have been designed and tested. This work did lead to a new type of an industrial disintegrator for the treatment of agricultural wastes. According to this design the machine was manufactured in a plant in Tallinn by a contract of a Spanish Company. It was tested and balanced by the group in Tallinn and exported for field tests to Sevilla, Spain.

The future task is to test and adjust the machine to different woody and herbaceous and maybe other materials. The developed disintegration grinder has a good chance to find increased application in rather wide areas.

Beside the mentioned two key persons there is a post graduate student involved.

### **Publications**

The self-assessment report lists 7 publications starting at 1996; several of them were published recently and one will appear in 2000. Most of them have been presented at recognized international conferences.

### **Research and Development**

The people have a great expertise in this very difficult area. By all means the results of research and development are new and of high quality. Of course, this group consisting of three people forms compared to the entire company just a small part. It is also very much dependent on the knowledge of the two key persons. The work, however, is more or less unique and recognized on an international level.

### **Competence of the Research Group**

As already mentioned the competence is excellent. There is a good chance that their work and results find besides Spain other international partners. If one considers the size of the group it is definitely worthwhile to continue with their project.

## **Part III**

# **General Recommendations**

The Team offers the following recommendation to Cybernetica and to other related bodies. The parties should view these recommendations as suggestions from colleagues. The Team has not given these recommendations in any order of priority and all concerning bodies may consider them for general improvements.

- The research and development work at the company has a good international reputation. Nevertheless, there is almost no joint research carried out between other research institutions, and there are only few joint research publications. The Team strongly recommends to intensify the co-operation with other research centers of similar interests.
- About half of the research staff are Master or Ph.D. students and the company has created very good working conditions for them. On the other hand, completion of a thesis takes time which is not in the interest of the company. Therefore we recommend the company to create conditions for Master and Ph.D. students to finish their theses at a reasonable time.
- The Team appreciates the work done by the company in developing new devices (disintegrators, navigation and surveillance systems etc). However, in some cases it seems that the company does not have a clear vision how the production should be

launched. For marketing data security products, a spin-off company Privador was established. However, for other developed devices there are no real partners for production and marketing.

- Looking at the budget of the company it seems to the Team that the company did not use other support (for example, the Estonian Innovation Foundation, EU funds etc.). The Team recommends the company to look for additional financing.
- The company spends about 10% of its income for research. This enables them to start with new research directions which the current competence based targeted financing would not allow. Therefore the Team recommends research financing bodies to create funds which will be given directly to the research institutions for starting research in new directions.
- It would be worthwhile to think it over to transfer the ownership of the company from the Ministry of Education to the Tallinn Technical University; in this case more technical and scientific expertise is involved.

## Part IV

### **Accreditation Conclusions**

1. The research staff forms a healthy organization: a big number dedicated young researchers led by experienced and well-known professionals.
2. The company has created motivating conditions for productive work e.g. a friendly atmosphere, excellent working conditions, relevant and challenging research problems and adequate salaries.

## Part V

### **Recommendations**

Evaluation judgement of research fields Cryptography and Datasecurity, Expert Systems Technology, Balancing Dynamics in Cybernetica Ltd.

***Good***

The Team has based its decision on the information received, the outcome of the accreditation visit, and the findings reported in Part II.