CORAS - A Framework for Risk Analysis of Security Critical Systems

Ketil Stølen
SINTEF Telecom and Informatics
P.O.Box 124 Blindern, N-0314 Oslo
E-mail: Ketil.Stoelen@informatics.sintef.no

Abstract[1]

CORAS is a research and technological development project under the Information Society Technologies (IST) Programme (Commission of the European Communities, Directorate-General Information Society). CORAS started up in January 2001 and runs until July 2003. The CORAS main objectives are as follows. (1) To develop a practical framework, exploiting methods for risk analysis developed within the safety domain, semiformal description methods (in particular, methods for object-oriented modeling), and computerized tools (for the above mentioned methods), for a precise, unambiguous, and efficient risk analysis of security critical systems. (2) To apply the framework in security critical application domains. (3) To assess the applicability, usability, and efficiency of the framework. (4) To promote the exploitation potential of the CORAS framework.

This paper presents the philosophy on which CORAS builds, its main hypothesis, and the more detailed goals and plans for the technical workpackages.

1. Introduction

Both users and vendors of information and communication technology have interests in a high level of security. Vendors need to establish trust and confidence in their products and services, and users need to protect their information and trust their vendors. Although all systems need some level of security, we believe that systems for e-commerce, medical and legal databases, financially critical systems, centralized as well as web hosting, are particularly security critical.

We appreciate the need for improved methods of identifying and analyzing possible security threats. We also recognize that the traditional models of trust between vendors and buyers fail to live up to the requirement for an electronic market place, where anonymous transactions cross territorial and legal boundaries. Whereas alternative quantification of trust based on systematic methods for threat identification and risk analysis may offer better evaluations of transaction risk in this environment. The risk analysis approach aims to control risk; it is a rigorous balancing process of determining how much and what kind of security to incorporate in light of business needs and acceptable levels of risk.

Risk analysis has already been proven as a powerful tool in ensuring safety in transportation, production and industry. However, the increasing complexity of today's systems urges the improvement of existing methods of analyzing systems and their security specification in order to increase the likelihood that all possible security threats are taken into consideration. Consequently, the demand for a more orderly and formal treatment of risks is increasing.

By applying semiformal methods we aim to alleviate, and in some cases eliminate, ambiguities and other difficulties in specifying security requirements. By applying object-oriented modeling methods we expect to achieve tractable system descriptions and therefore improve the use of risk analysis methods. This combination will eventually lead to assuring the realized security policy.

CORAS [1] aims to adapt, refine, extend, and combine methods for risk analysis, semi-formal description methods – in particular, methods for object-oriented modeling (e.g., UML [2], SDL [3], MSC [4]), and computerized tools to build a specialized RM-ODP [5] inspired framework targeting risk analysis of security critical systems.

The objective of this paper is to give an overview of the CORAS project. We present and motivate the ideas on which CORAS builds and how these ideas are to be implemented. The remainder of the paper is divided into eight sections. Section 2 describes the CORAS consortium. Sections 3 and 4 present the CORAS

[1] *The paper has been compiled from the technical annex of the CORAS contract with the Commission of the European Communities. The role of Ketil Stølen in the preparation of this paper has mainly been that of an editor. The technical annex has been prepared by the representatives of the ten CORAS partners.*

objectives and main hypothesis, respectively. Work within CORAS is divided into four technical workpackages. They are described in Sections 5 through 8. Section 9 provides references.

2. The CORAS partners

The CORAS consortium consists of two British, one German, two Greek, and five Norwegian partners; in alphabetic order:

- Computer Technology Institute (CTI) – Greek non-profit, financially and administratively independent research organization;
- Institute for Energy Technology (IFE) – Norwegian non-profit, independent research foundation;
- Intracom SA – the leading Greek telecommunications company;
- National Centre for Telemedicin (NCT) – centre of competence coordinating Norwegian telemedicine research and development;
- Norwegian Computing Centre (NR) – Norwegian non-profit, independent research foundation;
- Queen Mary and Westfield College (QMW) – college of the Federal University of London, UK;
- Rutherford Appleton Labs (RAL) – principle site of the UK Central Laboratory of the Research Councils (CLCR) supporting and participating in research projects in a wide range of disciplines;
- SINTEF – Norwegian non-profit, independent research foundation;
- Solinet – German software and hardware development company specializing in ready-to-run telecommunication solutions;
- Telenor – the major Norwegian telecommunications operator.

Telenor and SINTEF are responsible for the administrative and scientific coordination, respectively.

3. The CORAS objectives

In recognition of the fact that information and communication technologies are becoming a dominant part of people's everyday life, the CORAS consortium, representing users and vendors of information and communication technology, value the importance of establishing trust and confidence in their products and services. Beyond and above the obvious market advantage, building consumer confidence and trust in information and telecommunication products is nowadays becoming a social matter.

To implement security in a way that meets business needs cost-effectively, both in the short term and as enterprise needs expand, is a major challenge for users and vendors of information and communication technology in Europe and world-wide. In order to meet this challenge, we need to improve the existing methods of identifying and analyzing possible security threats, of developing security specifications, and of designing security policies. We consider systematic methods for threat identification and risk analysis to be the best candidate for this.

CORAS intends to develop a base framework applicable to security critical systems that will supply customizable, component-based road maps to aid the early discovery of security vulnerabilities, inconsistencies and redundancies. The CORAS main objectives are:

- to develop a practical framework for precise, unambiguous and efficient risk analysis, by exploiting the synthesis of risk analysis methods with semiformal specification methods (in particular, methods for object-oriented modeling) and computerized tools, in order to improve the risk analysis of security-critical systems;
- to assess the applicability, usability and efficiency of the framework by extensive experimentation in the fields of e-commerce and telemedicine;
- to investigate its commercial viability and pursue its exploitation within relevant market segments, while playing an influential role in standardization organizations.

The CORAS framework will provide a general and modular approach to risk analysis of security-critical systems in a manner that gives comprehensibility, precision, flexibility, ease of automation, and ease of verification and validation. It will be useful in developing new systems as well as in maintaining and improving legacy systems. The framework will comprise:

- Methods for precise and unambiguous evaluation, description, and definition of the analyzed system and the risks to which it is exposed.
- Methods for the accurate specification of security requirements, which form the basis for establishing security policy.
- The adaptation, extension, and specialization of RM-ODP into a framework aiming at the modeling and risk analysis of security critical systems.
- Libraries of standard modeling elements specialized towards the two trial domains.
- Methods for consistency checks of risk analysis results.
- Methods for the comprehensible presentation and communication of the risk analysis results and the security requirements, thus making possible the qualitative modeling, management and documentation of risks.

An overview of a potential exploitation of the CORAS framework in the analysis and design of security critical systems is illustrated by the figure below.

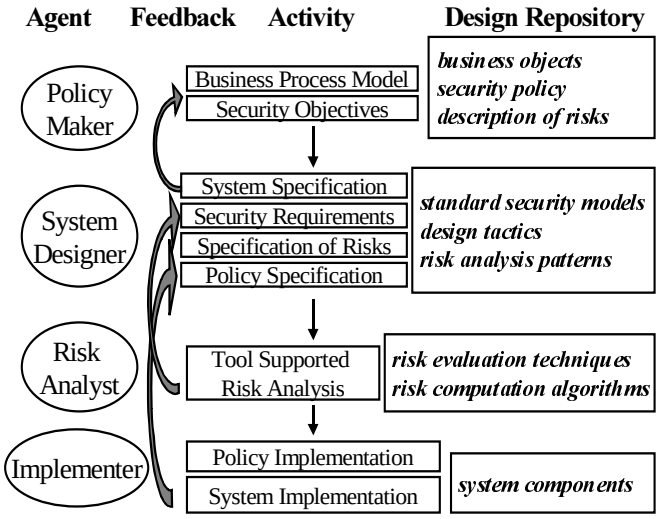

Figure 1: Potential exploitation of the CORAS framework

4. The CORAS main hypothesis

CORAS is based on the hypothesis that a carefully designed framework obtained through adapting, refining, extending, and combining existing

- methods for risk analysis;
- semiformal description methods within an RM-ODP setting;
- computerized tools

will improve on state-of-the-art methodology for risk analysis of security critical systems. To try out this hypothesis the technical project work has been divided into four major workpackages. Three of these - described in Sections 5, 6 and 7, respectively – are concerned with building the framework. The fourth – described in Section 8 – is intended to provide feedback and test the hypothesis in two large trials, one within telemedicin and one within e-commerce.

5. Risk analysis

Methods for risk analysis like

- FMEA/FMECA - failure modes, effects and criticality analysis [6];
- FTA - fault tree analysis [7];
- HAZOP - hazard and operability analysis [8];
- Markov analysis [9];
- GMTA – goals, means, task analysis [10].

have partly been developed for the process industry. They have also been used more broadly to analyze and evaluate safety critical systems. For example, IFE, in co-operation with the Norwegian company Scandpower, has successfully employed this kind of methods to identify and analyze safety risks in a commercial train-leader communication system. There has recently also been attempts to employ the same kind of methods to evaluate security critical systems. Telenor, one of the CORAS industrial partners, has in fact been involved in this.

Qualitative methods, such as FMECA and HAZOP, lack the ability to account the dependencies between events, but are effective in identifying potential hazards and failures within the system. The tree-based methods take into consideration the dependencies between each event. However, to fully exploit the above-mentioned methods, together with other risk analysis methods, in the analysis of security critical systems there is a clear need for further specialization. For example, we are not aware of an integrated approach to security modeling and risk analysis.

CORAS will address the deficiencies of conventional risk analysis methods within the area of security critical systems and, in particular, address the integration of risk analysis methods with state-of-the-art modeling paradigms. Emphasis will also be put on a discussion of the risks porting quantified methods of risk assessment to the security domain.

The innovation of the risk analysis workpackage consists in:

- Tuning risk analysis methods that have been developed mainly to ensure safety in transportation, production and industry to identify and analyze treats and hazards in security critical systems.
- Adapting these risk analysis methods to make full use of methods and CASE-tools for object-oriented modeling, design and analyses (e.g., UML, SDL, MSC).
- Designing patterns or guidelines to support the risk analysis of semiformally specified security critical systems, also taking into account the practical experience with integration and trials in the telemedicine and e-commerce sectors.
- Developing methods for presentation of risk analysis results thereby making possible the qualitative modeling, management, and documentation of risks.
- Designing procedures for consistency checking of results from risk analysis.

6. Modeling and specification

In order to properly evaluate whether a system is sufficiently secure we need a full understanding of all security relevant aspects – these aspects are of course not

confined to technical issues only, they are also concerned with the organizations and work processes in which the system is embedded. Viewpoint oriented modeling is a way of taking care of this. RM-ODP represents state-of-the-art for viewpoint oriented modeling of distributed systems. Although RM-ODP provides specialized security-related functions there is need for further specialization to fully meet the requirements of security-critical distributed systems.

RM-ODP offers general guidelines for the structuring and organization of system documentation. RM-ODP does not offer techniques and methods for writing the various specifications of which the system documentation consists. We distinguish between four kinds of specification methods:

- *Informal Description Methods* (IDMs): Is mainly based on natural language descriptions.
- *Semi-Formal Description Methods* (SFDMs): Look formal, but are called semi-formal because the grammar and/or meaning of specifications expressed with the help of these methods are not fully defined. Examples of SFDMs are OMT [11], UML, Booch [12], and ROOM [13].
- *Formal Description Methods* (FDMs): The FDMs differ from the SFDMs in that their specifications have a well-defined grammar and a meaning captured in some well-understood mathematical structure. Well-known examples of FDMs are SDL, MSC, and LOTOS [14].
- *Formal Description and Development Methods* (FDDMs): The FDDMs differ from the FDMs in their support for the logical deduction of implementations from specifications. Any FDDM contains one or several FDMs for specification purposes – for example, one FDM for requirements capture and another FDM for design. Typical examples of FDDMs are VDM [15], Z [16], B [17], Unity [18], and TLA [19].

Within the FDM and FDDM communities there is currently much interest in formal modeling, verification and analysis of security related issues. Many approaches have been proposed. Most of these are based on conventional FDMs and FDDMs like those mentioned above. There are however also some more recent approaches like for example the Ambient Calculus of Cardelli/Gordon [20] and the Spi-calculus of Abadi/Gordon [21] that give more direct support for security.

The obvious disadvantage of IDMs is lack of precision. Moreover, the possibilities for tool-support are of course restricted. Almost any commercial software/developer uses SFDMs in one form or another. Graphical FDMs like SDL and MSC are also popular. On the other hand, more mathematical FDMs and the FDDMs (in the literature often referred to as formal methods) have been very slow at gaining industrial acceptance. Finney/Fenton [22] summarize the situation as follows:

- Most formal methods have not penetrated far from their academic roots.
- Very few companies in the world use any formal methods systematically.
- Most major IT companies have no plans to use formal methods.
- The rare industrial uses of formal methods are restricted to formal specification; there is almost no evidence of any serious attempt at formal development or program proof. Thus, the original raison-d'etre of formal methods has not been seriously tested.

Today, five years later, the summary of Finney/Fenton remains valid. The CORAS project will therefore concentrate on SFDMs and graphical FDMs – in particular, on object-oriented methods in the style of UML that is currently dominating the area of semiformal modeling.

UML has in our opinion its main strengths in the creation of design models for traditional object-oriented systems, although trying to cover a much wider set of models and domains. To obtain sufficient support for the specification of security related aspects we strongly believe it is necessary to combine conventional UML diagrams with other modeling methods and paradigms.

CORAS will address the deficiencies of RM-ODP and object-oriented modeling technology and provide a specialized RM-ODP inspired modeling framework targeting risk analysis of security critical systems. The main innovation of the modeling and specification workpackage consists in the development of an RM-ODP inspired framework based on semi-formal description methods – in particular, methods for object-oriented modeling (e.g., UML, SDL, MSC) - well-suited to specify security-critical system components. In particular, the innovation involves:

- Giving detailed recommendations with respect to which security-relevant aspects should be specified within which ODP viewpoint.
- Within each relevant viewpoint, defining specialized models well-suited for the various risk-analysis methods considered.
- Defining libraries of standard specification fragments.
- Developing new security-oriented transparencies inspired by the already existing RM-ODP distribution transparencies.
- Characterizing the relationships between different security models and between security models and implementations. Based on the characterization mentioned above:

1. designing pragmatic rules, patterns, and procedures for checking the consistency of models;
2. providing rules and patterns allowing risk analysis carried out within one viewpoint or model to be exploited to simplify, guide or improve the effectiveness of risk analysis within other viewpoints or models;
3. providing patterns for modular and compositional maintenance of risk analysis results;
4. providing scenario-driven design tactics in order to facilitate the specification of security policies using the rules, patterns, and procedures mentioned above.

- Providing methods for efficient and comprehensible communication of security requirements to policy makers.

7. Integration and tool support

There are numerous CASE-tools providing comprehensible support for semiformal modeling in an object-oriented style. Rational Rose (Rational), ObjectTime (recently bought up by Rational), SDT (Telelogic), ObjectGEODE (earlier Verilog, today Telelogic), Rhapsody (i-Logix) and STATEMATE (i-Logix) are well-known. Tools of this type, however, give little or no direct support for the kind of risk analysis addressed by CORAS.

There are also a number of specialized computerized tools for risk analysis. Well-known examples are RAMS Software tools (Item Software), Toolkit for RAMS (IsographDirect), and CARA Fault-tree (DNV). Unfortunately, these tools are just as weak when it comes to modeling as the modeling tools, mentioned above, are weak when it comes to risk analysis.

The CORAS project intends to address this deficiency by combining and integrating techniques, methods, and computerized tools from the until today relatively unrelated areas of risk analysis and semi-formal modeling to provide a specialized framework supporting the identification and analyses of hazards in the development and maintenance of security critical systems.

The innovation of the integration workpackage consists in developing a general process supporting identification and analysis of security hazards based on the approaches to risk analysis and modeling described above. In particular, innovation involves the construction of

- templates,
- rules, and
- guidelines

for how to exploit the RM-ODP inspired framework and the various CORAS methods and computerized tools in the development and maintenance of security critical systems. This process will not be built from scratch but should rather be seen as a refinement of an already well-established systems development and maintenance process like, for example, the Rational Unified Process [23]. The innovation also consists in proposing a tool-chain providing computerized support for this process.

8. Trials

The lack of experimental evidence for claims is a general problem within computer science. Tichy points out [24]: “There are plenty of computer science theories that haven’t been tested. For instance, functional programming, object-oriented programming, and formal methods are all thought to improve programmer productivity, program quality or both. It is surprising that none of these obviously important claims have ever been tested systematically, even they are 30 years old and a lot of effort has gone into developing programming languages and formal techniques.”

That the level of experimental evidence is much lower in computer science than in more classical sciences has been confirmed by several studies. In a random sample of all the papers the ACM published in 1993, Tichy et al. [25] found that 40 percent of the papers with claims that needed empirical support had none at all. In software related journals, this fraction was 50 percent. The same study also analyzed a non-computer science journal, Optical Engineering, and found that the fraction of papers lacking experimental evidence was merely 15 percent. Zelkowitz et al [26] found similar results.

The CORAS project takes this criticism seriously and will try to provide empirical evidence for the quality of the CORAS framework through practical trials in the domains of e-commerce and telemedicine. More explicitly, the objectives of the CORAS trials are to

- validate the generality and applicability of the CORAS framework through trials in security critical application domains;
- demonstrate the applicability, usability and efficiency of the CORAS framework in
  1. modeling the relevant security-critical aspects of the chosen trial systems;
  2. performing risk analyses based on the models of security-critical aspects;
  3. recommending improvement of security policies on the basis of risk analysis results;
- provide assessment feedback to the three other technical workpackages described above;
- identify important security issues for the telemedicine and e-commerce application areas.

8.1. The CORAS telemedicine trial scenario[2]

The telemedicine platform chosen for the telemedicine trial is the HYGEIAnet, the regional Health Telematics Network of Crete. It is implemented as a Virtual Private Network (VPN) that isolates the HYGEIAnet as well as the applications using its services from the outside world (i.e., the Internet) by means of firewalls. On a second level, security is obtained through cryptographic primitives and protocols that provide data encryption, digital signatures, public key cryptography, key generation etc. It is a fairly complex system that uses distributed patient record systems accessible over the Internet, and it integrates different communications infrastructures. Sharing and communication of patients' records is based on a Patient Clinical Data Directory (PCDD), a middleware platform that provides clinical information based on distributed electronic health care records maintained by autonomous information systems in the HYGEIAnet. The security aspects of the system are obvious: confidentiality, availability, integrity, authentication and non-repudiation, and thus it will be useful for the CORAS project to test its framework on this scenario.

Using the CORAS framework, we will model security relevant aspects of the HYGEIAnet platform and applications, and perform risk analysis on the resulting models. This will be done in an iterative manner, providing feedback to the developers of the CORAS platform between the iterations. We will consult developers and managers of the HYGEIAnet, as well as medical doctors using the applications and services, to get feedback from different kinds of users on the applicability, usability, and efficiency of the framework.

8.2. The CORAS e-commerce trial scenario

The CORAS methodology will also be practically demonstrated and evaluated within the e-commerce domain. This domain is a commercially popular area where personal profile data and economic aspects need to be securely manipulated. This imposes a challenge in manifesting the build and provision of applications that can guarantee security based on the usage of advanced methodology practices prescribed by CORAS. To this respect, an existing e-commerce system will be considered in which the CORAS framework will be applied with the view to identify, analyze and document involved risks. The output of this exercise will provide valuable input in the process of defining security policies to be implemented in the system.

[2] *The final agreements with the owners of the network had not been signed when this paper was completed.*

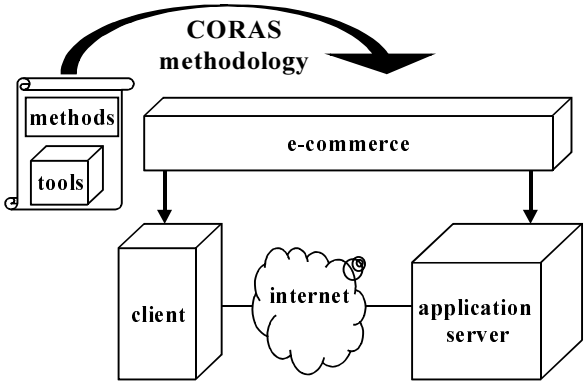

Figure 2: E-commerce trial components

CORAS will actually use an existing prototype software solution developed within the (EU/ACTS) ACTIVE project. The platform supports integrated retail services, providing an intelligent interface upon which the involved players (retailers, suppliers, and consumers) establish a tied and trusted relationship.

The main components of the system are:

- *Home Shopping Tool (HST)* for secure home shopping that provides consumers with an intelligent support for product filtering and targeted recommendation based on consumer profile. At the same time it acts as a POS (Point Of Sales) for order and payment, integrated with the retailers legacy systems, where the consumer can opt for his preferred virtual store environment.
- *Consumer Behavior Tool (CBT)* that monitors consumer behavior and defines consumer profiles that will support providers to apply targeted promotion techniques such as coupons, e-mail discount alerts, direct compensation for ad viewers, and sweepstakes. At the same time it applies direct market research through electronic questionnaires and product rating.
- *Advertising Tool (AT)* that allows the suppliers to advertise their products in the virtual shop to a well-defined target consumer group. In addition, it provides alternative advertising schemes that guide providers to display product information based on standard presentation templates or use specific Internet advertising techniques (web site navigation, video display etc.) in a cost scaleable way, based on multimedia and electronic forms technologies.

The trial scenario, to be considered and concretely elaborated during the initial phases of the trial, will concern trading of health-care products like pharmaceutical and para-pharmaceutical products and surgery supplies. Trading implies (personalized on the

basis of collected consumer data) advertising and promotion, browsing, ordering, and purchasing of traded goods. The most security critical aspects of such e-commerce scenarios will be considered by the CORAS trial. Such aspects include consumer profiling, ordering, and payment. Relevant and appropriate test cases in connection with risk analysis will be defined to enable the identification of possibly involved security risks concerning service availability, data integrity, secure connection, secure transaction-payments, confidentiality, protection of personal data, authentication, authorization, non-repudiation. The spectrum of security aspects to be actually considered will be defined in the first phases of the trials during which security requirements will be collected in consultation with platform users and developers.

The e-commerce trial will apply the CORAS framework to model the chosen system aspects in an ODP-inspired manner. The existing system implementation is JAVA based and runs on PC. It is a centralized implementation that will be made distributed in the context of CORAS. Security issues, including risks stemming from the introduction of distribution in the modeled system will be analyzed. The results of this risk analysis in combination with security requirements expressed by the e-commerce platform developers and users will provide recommendations for the definition of security policies to secure the system. The results will also indicate the security level offered by the system and the efficiency of the CORAS framework when applied to the specific application domain. Through this process, the tools, risk analysis and modeling methods of the CORAS framework will be assessed and relevant feedback will be provided to the other three technical workpackages of the CORAS project.

9. References

[1] CORAS: A platform for risk analysis of security critical systems. IST-2000-25031, 2000. (http://www.nr.no/coras/)

[2] UML proposal to the Object Management Group, Version 1.3, 1998.

[3] Recommendation Z.100 - CCITT Specification and Description Language (SDL). ITU, 1993.

[4] Recommendation Z.120 - Message Sequence Chart (MSC). ITU, 1996.

[5] J. R. Putman. Architecting with RM-ODP. Prentice Hall, 2001.

[6] A. Bouti, D. Ait Kadi. A state-of-the-art review of FMEA/FMECA. International Journal of Reliability, Quality and Safety Engineering 1:515-543, 1994.

[7] IEC 1025: Fault tree analysis (FTA), 1990.

[8] F. Redmill, M. Chudleigh, J. Catmur. Hazop and Software Hazop. Wiley, 1999.

[9] B. Littlewood. A reliability model for systems with Markov structure. Appl. Stat. 24:172-177, 1975.

[10] E. Hollnagel. Human reliability analysis: context and control. Academic Press, 1993.

[11] J. Rumbaugh, M. Blaha, W. Premerlani, F. Eddy, W. Lorensen. Object-oriented modelling and design. Prentice Hall, 1991.

[12] G. Booch. Object-oriented analysis and design with applications (second edition). Benjamin/Cummings Publishing Company, 1994.

[13] B. Selic, G. Gullekson, P. T. Ward. Real-time object-oriented modelling. Wiley, 1994.

[14] Information processing systems - Open systems interconnections - LOTOS - A formal description technique based on the temporal ordering of observational behaviour. ISO/IEC 8807, ISO, 1989.

[15] Information technology - Programming languages, their environments and system software interfaces - Vienna Development Method --- Specification language. ISO/IEC 13817, ISO, 1996.

[16] J. Spivey. Understanding Z. Cambridge University Press, 1988.

[17] J.-R. Abrial. The B-book. Cambridge University Press, 1996.

[18] K. M. Chandy, J. Misra. Parallel program design. Addison-Wesley, 1988.

[19] L. Lamport. The temporal logic of actions. ACM Transactions on Programming Languages and Systems. 16:872-923,1994.

[20] L. Cardelli, A. D. Gordon. Mobile ambients. Theoretical Computer Science 240:177-213, 2000.

[21] M. Abadi, A. D. Gordon. A Calculus for cryptographic protocols: the Spi calculus. Information and Computation 148:1-70, 1999.

[22] K. Finney, N. E. Fenton. Evaluating the effectiveness of using Z: the claims made about CICS and where we go from here. Journal of Systems Software 35:206-219, 1996.

[23] I. Jacobson, G. Booch, J. Rumbaugh. The unified software development process. Addison-Wesley, 1998.

[24] W. F. Tichy. Should computer scientists experiment more? IEEE Computer 31: 32-40, 1998.

[25] W. F. Tichy, P. Lukowics, P. Prechelt, E.A. Heinz. Experimental evaluation in computer science: a quantitative study. Journal of Systems Software 28: 9-18, 1995.

[26] M. V. Zelkowitz, D. R. Wallace. Experimental models for validating technology. IEEE Computer 31: 23-31, 1998.