COST-247 Action

COST-247: Verification and Validation for Formal Descriptions

Final Report

December 24, 1997

A Survey of Value Passing Process Algebras

Matthew Hennessy

School of Cognitive and Computing Sciences
University of Sussex
Falmer, Brighton
Sussex BN1 9QH
United Kingdom
Email: matthewh@cogs.susx.ac.uk
Tel: +44 1273 678 195
Fax: +44 1273 671 320

Most of the traditional verification methods for process description languages rely on the fact that the underlying transition systems are finite branching. If processes are allowed to send and receive messages or values from an infinite data set then this is rarely the case. However if we work with "symbolic transition systems" as opposed to the usual concrete ones then many of the standard methods can still be applied. This talk will survey recent joint work with H. Lin and X. Liu on this symbolic approach to message-passing processes. This will include a theory of symbolic bisimulations, sound and complete proof systems for mesage-passing process calculi and a logical characterisation of bisimulation equivalence in terms of a first-order modal logic.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Web links: `http://ida.dcs.qmw.ac.uk/authors/H/HennessyM`

A Timed Full LOTOS with Time/Action Tree Semantics

Tommaso Bolognesi

CNR-CNUCE
36, via S. Maria
I-56100 Pisa
Italy

Tel: 39 50 593319
Fax: 39 50 589354
E-mail: bolog@fdt.cnuce.cnr.it

Starting from the current Full LOTOS standard, which integrates two components dealing, respectively, with process behaviours and data, we address the problem of designing a minimal extension of the language offering a satisfactory integration of a third component: the time dimension. We present here a Timed Full LOTOS which achieves this goal by simply adding (two variants of) a powerful time-related operator to the current standard. An operational semantics is provided, consisting of two sets of inference rules, one for instantaneous action transitions and the other for time passing transitions. With respect to the original Full LOTOS operators, the rules in the first set are precisely those found in the standard, while the rules in the second set are trivial, and derive from an assumption of time determinism and globality. The complexity of the timed extension is thus confined into the inference rules of the new time-related operators.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

A Formal Definition of Time in LOTOS

Luc Leonard, Guy Leduc

Universite de Liege
Systemes et Automatique
Institut Montefiore, bat. B28
B4000 Liege
Belgium
Tel: 32 43 66 49 92
Fax: 32 43 66 29 89
E-mail: leonard@montefiore.ulg.ac.be

A time extended version of LOTOS, denoted ET-LOTOS, is proposed for the modelling of real-time behaviours. The language is first presented informally and applied to many small examples of sequential and concurrent systems. Then the formal semantics is given in two steps: on Basic ET-LOTOS and then on full ET-LOTOS. Several equivalence relations are defined and many properties (equivalence laws, expansion theorems, ...) are presented. The upward compatibility of ET-LOTOS w.r.t. LOTOS is also discussed.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

Web links:
`http://www-run.montefiore.ulg.ac.be/publications/papers/abstract-RS95-05.html`

Web links: `http://www-run.montefiore.ulg.ac.be`

A Timed LOTOS Extension

Juan Quemada

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain
Tel: +34 1 3367331
Fax: +34 1 3367333
E-mail: jquemada@dit.upm.es

T-LOTOS, is a timed extension of LOTOS is described where the semantics is described in the form of timed-action trees. In timed-action trees the passing of time is represented as time stamps of actions, being each time stamp the time passed from the previous action occurred. Timed-action trees and Time/Action trees can be formally related by mapping B -at-¿ B to B -t-¿ B, B-a-¿ B (and viceversa). A formal framework for verifying timed systems is provided based on timed tests, by assigning a precise timing to the tests and observations performed.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Web links: `http://www.dit.upm.es/~quemada/`

A failures semantics for timed LOTOS

Steve Schneider

Royal Holloway, University of London
Egham, Surrey, TW20 0EX, UK
E-Mail: steve@dcs.rhbnc.ac.uk
tel: +44 1784 443431
fax: +44 1784 439786

Timed CSP has a denotational semantics in terms of timed failures. In this talk we investigate how this approach to semantics may be applied to a timed version of LOTOS, while remaining consistent with its operational semantics. It turns out that timed failures alone are not adequate, and that an additional component is required in the semantics in order to deal with operators that are sensitive to internal actions. The resulting denotational semantics is shown to be the weakest congruence stronger than trace equivalence. We also discuss the relationship with other approaches to timed LOTOS.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Web links: `http://www.dcs.rhbnc.ac.uk/research/formal/steve.html`

A Timed Process Algebra for Specifying Real-Time Systems

Sergio Yovine

Verimag
Centre Equation
2, avenue de Vignate
F-38610 Gieres
FRANCE

tel : +(33) 4 76 63 48 48
fax : +(33) 4 76 63 48 50
E-mail: Sergio.Yovine@imag.fr

We present the algebra of timed processes ATP for specifying the behavior of real-time systems. ATP introduces several timed constructs such as delayable actions, timeouts and watchdogs. The formal semantics of ATP is given in terms of labeled transitions systems where time passing is modeled by transitions labeled with the amount of time elapsed. We present a method for translating ATP into timed graphs which are automata extended with a finite set of real-valued clocks.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

The Tick-Tock Case Study for the Assessment of Timed Formal Description Techniques

L. Leonard, G. Leduc, A. Danthine

Institut d'Electricite Montefiore, B28
University of Liege
B-4000, Liege 1, Belgium
Email: leduc@montefiore.ulg.ac.be
Tel: +32 4 3662698
Fax: +32 4 3662989

A case study is proposed for the assessment of timed FDTs. It consists of a protocol composed of two entities and an underlying service provider, whose behaviour is mainly based on various timing constraints such as time-out, isochronism, rate-control, The selection of the mechanisms was guided by the two following characteristics:- Realism: The selected mechanisms have been inspired by similar and existing protocol mechanisms or service facilities, but they have been (over)simplified to focus the case study on the timing constraints. - Temporal modelling facilities: The specificity and the variety of the timing constraints are intended to assess whether timed FDTs have enough power and flexibility to tackle a maximum number of aspects of timed behaviours. Of course, not all the possible timed behaviours that may exist in protocols are explored, but a broad spectrum of them is covered.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Web links:
`http://www-run.montefiore.ulg.ac.be/publications/papers/abstract-R94-07.html`

Web links: `http://www-run.montefiore.ulg.ac.be`

Case-studies using Timed Full LOTOS

Tommaso Bolognesi

CNR-CNUCE
36, via S. Maria
I-56100 Pisa
Italy

Tel: 39 50 593319
Fax: 39 50 589354
E-mail: bolog@fdt.cnuce.cnr.it

Abstract Specifications of a Railroad Crossing system and of the so called Tick-Tock service are introduced for illustrating the Timed Full LOTOS with Time/Action tree semantics of a companion presentation.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Examples of the Use of ET-LOTOS

Luc Leonard

Universite de Liege
Systemes et Automatique
Institut Montefiore, bat. 28
B4000 Liege
Belgium

Tel: 32 43 66 49 92
Fax: 32 43 66 29 89
E-mail: leonard@montefiore.ulg.ac.be

To justify the design choices of ET-LOTOS and to prove their advantages, the specification of two case studies is presented: a subset of the Tick-Tock case study, completed with some additional difficulties, and the rail road crossing example.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Web links: `http://www-run.montefiore.ulg.ac.be`

Case-studies using T-LOTOS

Juan Quemada

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain
Tel: +34 1 3367331
Fax: +34 1 3367333
E-mail: jquemada@dit.upm.es

The rail road crossing example is specified using T-LOTOS by specifying the system as three components: the gate, the controller and the rail-sensor part. In order to illustrate a stepwise refinement design approach in a timed context, the service offered by the system, when the internal communication among parts is hidden is also presented. The specification of some parts of the Tick-Tock protocol are also given.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Web links: `http://www.dit.upm.es/~quemada/`

Case studies using TCSP

Jim Davies

University of Reading
Department of Computer Science
P.O. BOX: 225
UK-PG6 2AY Whiteknights Reading
United Kingdom

Tel: 44 1734 318611
Fax: 44 1734 751994
E-mail: j.w.davies@reading.ac.uk

This talk begins with an introduction to the language and models of real-time CSP. This is followed by a series of examples which illustrate the relationship between real-time CSP and ET-LOTOS, a real-time extension of the LOTOS formalism. If time allows, the talk will end with a case study: the Tick-Tock protocol.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Kronos: A Tool for Verifying Real-time Systems

Sergio Yovine

Verimag
Centre Equation
2, avenue de Vignate
F-38610 Gieres
FRANCE

tel : +(33) 4 76 63 48 48
fax : +(33) 4 76 63 48 50
E-mail: Sergio.Yovine@imag.fr

Kronos is a tool that performs symbolic model-checking for real-time systems. It reads a timed graph describing a real-time system and a TCTL formula specifying a requirement, and checks whether the timed graph satisfies the formula. Timed graphs are automata extended with a finite set of real-valued clocks, used to express timing constraints. TCTL is an extension of the temporal logic CTL that allows quantitative temporal reasoning. We first review the main theoretical results and then we show the performances obtained with Kronos in some case studies, in particular the Tick-Tock protocol.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Introducing Mobility in LOTOS

Elie Najm

Ecole Nationale Superieure des Telecommunications
46, rue Barrault
F-75013 Paris
France

Tel: 33 1 45817709
Fax: 33 1 45891664
E-mail: najm@res.enst.fr

The New Work Item on the extensions of LOTOS has established a list of desirable features that are candidates for incorporation in the language, and a list of requirements that E-LOTOS should aim to fulfil. One of these requirements is the ability of the language to describe concepts related to the Open Distributed Processing (ODP) framework. LOTOS is known not to address properly some of the modelling problems raised by modern distributed systems. One major issue is to describe the dynamic reconfiguration of components and the changing communication patterns that characterise ODP. The present contribution is a first attemp towards the introduction of mobility in LOTOS. It is aimed at enhancing the language while preserving its main advantages as a modular and concise specification technique. It draws upon research done in the area of mobile process algebras in general and upon Milner's pi-calculus in particular. The present text is not yet a finalised answer but is aimed at opening the technical discussion on the issue of mobility. It presents a Synchronous Mobile Calculus (SMC) a calculus which exhibits features common to LOTOS and the p-calculus.

This presentation has been given during the COST-247 WG1 Special Workshop on Extended Process Algebras (Brighton, United Kingdom, July 19–20, 1994).

COST-247 Working Group(s): 1

Thoughts on the future of algebraic types in LOTOS

Muffy Thomas

University of Glasgow
Dept. of Computer Science
UK-G12 8QQ Glasgow
United Kingdom

Tel: +44 141 330 4969
E-mail: muffy@dcs.glasgow.ac.uk

This talk discusses some of the requirements for a data type language in LOTOS, how ACT ONE meets them, and how other languages and constructs might better fulfill them.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1-2

A LOTOS Verification Case Study

Muffy Thomas

University of Glasgow
Dept. of Computer Science
UK-G12 8QQ Glasgow
United Kingdom

Tel: +44 141 330 4969
E-mail: muffy@dcs.glasgow.ac.uk

This talk presents the results of a case study of the high-level design of a control device for a dual-mode linear accelerator, based on the Therac-25. The specification language LOTOS is used throughout. First, a basic LOTOS design is developed, and analysed for safety properties using both property testing (with LOLA), reasoning with the cred relation (with PAM), and using the modal mu-calculus (with CAESAR toolkit). Second, state is added in the form of abstract data types as parameters to the processes. These model the shield and beam entities. This design is also analysed, using property testing and the modal mu-calculus. In each case, we discuss what can and can't be proved, the benefits of the tools, and the contribution of the exercise to the safety case.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1-2

CONCUR2: Datatypes and processes task

Alan Jeffrey

School of Cognitive and Computing Sciences
University of Sussex
Falmer, Brighton
Sussex BNI 9QH

Tel: 44 1273 678 526
Fax: 44 1273 678 188
E-mail: alanje@cogs.susx.ac.uk

CONCUR2 is a an ESPRIT Basic Research Action into calculi and algebras for concurrency. One of the tasks has been to investigate the use of datatypes in modelling concurrent systems. This talk will present an informal overview of the task, with a short summary of the methodologies investigated, and the results achieved. (Alan Jeffrey is the leader of this CONCUR2 task).

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1-2

Reachable state space analysis of LOTOS specifications

Alain Kerbrat

Verimag
Centre Equation
2, avenue de Vignate
F-38610 Gieres
FRANCE

tel : +(33) 4 76 63 48 48
fax : +(33) 4 76 63 48 50
E-mail: Alain.Kerbrat@imag.fr

We present a symbolic analysis technique for LOTOS programs with integer variables on which only linear expressions are allowed. The technique is applicable to models generated by the CAESAR compiler which are Petri nets extended with guarded commands. It allows to compute a predicate on variables characterizing the set of the reachable states or an upper approximation of it. Predicates are represented as systems of linear inequalities on program variables. We implemented a tool for performing the operations necessary for the analysis such as conjunction, disjunction, widening operation as well as comparison of predicates. The method is applied to two examples showing that non trivial relations between program variables can be discovered.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1-2

Computable data types for E-LOTOS

Charles Pecheur

University of Liege
Institut Montefiore B28
B-4000 Liege
Belgium

This presentation proposes a new semantical model for LOTOS data types, based on explicit distinction between constructors and functions and a deterministic evaluation function. This results in effectively computable data types and enhances modularity. We also define an associated type definition syntax, inspired from ML, and present some possible developments. We then discuss how equality can be defined: though some types (like sets) cannot be defined so that language-level equality matches the intended equivalence, quite convenient workarounds can be used. We show how the deterministic evaluation allows simpler specifications, and how modularity and abstractness can be enforced. Finally, we will address the compatibility of the proposed evaluation with existing simulation approaches like rewriting and narrowing.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1

Overview of the CAESAR.ADT abstract data type compiler

Hubert Garavel

INRIA Rhone-Alpes / Dyade
655, avenue de l'Europe
38330 MONTBONNOT ST MARTIN
FRANCE
tel: +(33) 4 76 61 52 24
fax: +(33) 4 76 61 52 52
E-mail: hubert.garavel@inria.fr

We present the architecture and functioning principles of the CAESAR.ADT compiler. CAESAR.ADT (automatically) translates a subset of the data part of LOTOS into executable C code. The class of accepted LOTOS programs is very similar to the class of "computable data types" described by Charles Pecheur. LOTOS sorts are translated into C types using algorithms that can select efficient data representations for common types such as enumerated types, records, integers, etc. LOTOS operations are translated into C functions using a pattern- matching compiling algorithm proposed by Schnoebelen, which compiles the equations into deterministic C code (basically "if-then-else's" and recursive function calls). We present the successive mutations of the compiler since 1988, its applicability to large-size case studies, and the on-going developments.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1

Web links: `http://www.inrialpes.fr/vasy`

About partial functions

Jean-Michel Hufflen

CRIN-CNRS INRIA Lorraine
BP 239 - F-54506
Vandoeuvre Cedex
France

Current address:
Laboratoire d'Informatique de Besancon
Universite de Franche-Comte
16, route de Gray
25030 BESANCON CEDEX
Tel: +33 3 81 66 64 52
E-mail: hufflen@univ-fcomte.fr

It is well known that partial functions are difficult to put in algebraic specifications. Several solutions to this problem have been proposed, and each has its advantages and drawbacks, from a theoretical as well as pratical viewpoint. In this talk, we survey these propositions—including partial algebras, error algebras, exception handlings, order-sorted algebras, label algebras—and discuss them.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1

Convenient notations everywhere with Rich Term Syntax

Charles Pecheur

University of Liege
Institut Montefiore B28
B-4000 Liege
Belgium

All "real" programming languages offer a convenient syntax for widely used values such as numbers, arithmetic operations, array subscripts, strings, etc. Instead of a list of particular operations with ad-hoc syntax, we propose to offer a richer general syntax for terms, that is independent of any particular type or value and is available for any new operation definition. The use of a particular syntactic form is thus completely uncoupled from any particular semantics. We then present, discuss and illustrate a collection of syntax forms: functional, infix (both already available in LOTOS), sequences, selectors and modifiers, structure builders, characters and strings, numbers. We also take account of the technical aspects involved in the syntax analysis of such forms.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1

The algebraic specification language LPG: presentation and assessment of the design choices

Didier Bert

CNRS, LSR-IMAG, Grenoble
BP 53
38041 Grenoble CEDEX
France
Email: Didier.Bert@imag.fr
Tel: +33 4 76 82 72 16
Fax: +33 4 76 82 72 87

In this talk, we shall introduce the main features of the algebraic and logic specification language LPG. This language was defined and implemented at the IMAG Institute in the years 1984-86 and revised in 1991. It was used to specify and to prototype several cases studies, particularly in ESPRIT projects. Main characteristics of LPG will be presented, like the underlying logic, the predefined objects, the module decomposition and structuring, the parameterization facilities. The stress will be put on the differencies between LPG and LOTOS and on the consequences of some design choices.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1

Web links: `http://www-lsr.imag.fr/Les.Personnes/Didier.Bert/`

The GLIDER language

Jean-Michel Hufflen

CRIN-CNRS INRIA Lorraine
BP 239 - F-54506
Vandoeuvre Cedex
France

Current address:
Laboratoire d'Informatique de Besancon
Universite de Franche-Comte
16, route de Gray
25030 BESANCON CEDEX
Tel: +33 3 81 66 64 52
E-mail: hufflen@univ-fcomte.fr

GLIDER is an algebraic specification language developed as part of an ESPRIT project. It is a two-level language, providing a semantic kernel and the whole of the language. On the one hand, this distinction allows users to write down specifications as simple as possible, on the other hand, specifiers can be ensured that the "semantic" form of their specification is what they mean exactly. In this presentation, we emphasize these facilities—inference of imported modules, libraries, enumerated types, etc.—and show how they are put into action.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1

Overview of the SALSA project

Didier Bert

CNRS, LSR-IMAG, Grenoble
BP 53
38041 Grenoble CEDEX
France
Email: Didier.Bert@imag.fr
Tel: +33 4 76 82 72 16
Fax: +33 4 76 82 72 87

SALSA was a project founded by the French ministry of industry to study and implement techniques for integrating various algebraic specification environments. The idea was to make various specification languages available for users and to be able to share the tools which have been developped independently for each language. In this talk, we give an overview of the integration techniques studied and/or implemented.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1

A monadic language for concurrent programming

Alan Jeffrey

School of Cognitive and Computing Sciences
University of Sussex
Falmer, Brighton
Sussex BNI 9QH

Tel: 44 1273 678 526
Fax: 44 1273 678 188
E-mail: alanje@cogs.susx.ac.uk

Moggi has proposed "strong monads" as an appropriate notion for the description of computations such as side effects and nondeterminism. This talk describes an extension of Moggi's monadic meta-language with higher-order concurrent features. The monadic type system makes it much easier to present a semantics for the language. There is also a translation of Reppy's Concurrent ML into the concurrent monadic meta-language, which preserves weak bisimulation.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1

Verification of a railway safety box

Jan Friso Groote

Centrum voor Wiskunde en Informatica
Specification and Analysis of Embedded Systems
P.O. Box 94079
1090 GB Amsterdam
The Netherlands
Email: jfg@cwi.nl
Tel. +31-20-5924232
Fax. +31-20-5924199

We formulate safety requirements for railyard control and model these using modal logic. We transform code used by the Dutch Railway Company to safeguard stations as well as the requirements into propositional logic and verify these using a propositional logical checker. In this way we have established safety of railway control at the stations Hoorn-Kersenboogerd and HeerHugowaard.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 2

Web links: `http://www.cwi.nl/~jfg`

Developments in the definition and verification of the Xpress Transfer Protocol (XTP)

Octavian Catrina

Institut National des Telecommunications (INT)
Les Epinettes
9, rue Charles Fourier
91011 EVRY cedex
FRANCE
E-mail: tavi@elcom.pub.ro

Description. XTP was originally designed as a transfer layer protocol (transport and network layers)[PEI92]. XTP functions can be dynamically configured, using a minimal and flexible set of simple mechanisms ("light-weight transport"), in order to offer efficient solutions for different user requirements and network characteristics. Significant changes of the protocol definition were decided at the last meeting of the XTP Forum (the organisation that promotes the protocol), in July 1994. The new revision of the protocol definition (4.0), restricts XTP to the transport layer and is still under development. ¡P¿ Aplication. XTP was aimed to provide high performance for a broad range of service requirements, in high speed networks: it offers support for distributed, transactional and multimedia applications and efficient transfer of bulk data. It is currently used in experimental distributed multimedia systems, in USA and Europe. ¡P¿ Validation technique. The protocol was specified in Estelle, according to the previous definition (3.6) and the brief description of the modifications, distributed after the meeting of the Forum. No service definition is available. The verification was made using a generic transport service, defined for this purpose, and a connectionless network service. The generic service provides control of the configuration options and allows to take advantage of the XTP features, for performing efficiently different service types. A configuration consisting of XTP entities and a model of its environment was extensively simulated for a typical set of scenarios, using Edb, the simulation tool of the Estelle Development Toolset [Budk92], [EDT]. The

fast and systematic production of scenarios was facilitated by the design of a "programmable" user, configured by Edb macros and observers. Verification automata, implemented with Edb observers, were used for checking individual mechanisms and the offered service, during the simulations. ¡P¿ Conclusion. This study was aimed to offer support to the current conception phase, by exploring the effects of the modifications and by identifying and evaluating solutions for the new situations that might appear. It showed that the possibility to shape the protocol mechanisms by observing and verifying the simulations, interactively and automatically, can be of great help during protocol design. The study also offered the opportunity to improve the methods for automatic verification during the simulations, working on a real-life protocol, and to identify functions to be added to Edb, in order to facilitate the implementation of the observers.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 2

Web links: `http://alix.int-evry.fr/~stan/edt.html`

Verifying mutual exclusion algorithms by reducing state spaces

Martti Tienari

Department of Computer Science
P.O.Box 26 (Teollisuuskatu 23)
FIN-00014 UNIVERSITY OF HELSINKI
Finland
Tel:+358 9 7084 4175
Fax:+358 9 7084 4441
Email: tienari@cs.Helsinki.FI

This is a case study of verifying safety properties in some concurrent systems using state transition system reduction methods. Reductions have been made with respect to trace-, cffd-equivalences as well as various bisimilarities. A set of mutual exclusion algorithms were considered. By suitable hiding of labels reduced systems, suitable for verification purposes, were of the size of 7.. 20 states, typically. Thus the verification could be done visually based on the pictures of the reduced systems.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 2

Web links: `http://www.cs.helsinki.fi/~tienari`

The MEIJE verification toolset: new tools, and pragmatics

Eric Madelaine

INRIA Sophia-Antipolis
2004 rte des Lucioles
BP93
06902 Sophia-Antipolis Cedex
France
email: Eric.Madelaine@sophia.inria.fr
Tel: (+33) 4 93 65 78 07
Fax: (+33) 4 93 65 77 65

We present the MEIJE Verification Tool Set, including the tools ATG, Mauto and FcTools. The Verification Tool Set provides means for: drawing and editing automata and hierarchical networks of automata; building finite automata from those drawings, or from programs in CCS, Meije, Lotos, or Esterel; perform this building in a compositional way, together with various notions of semantic minimizations and abstractions; display graphically the results, and extract diagnostic information from elements of the reduced models. We comment on various exemples and case studies, and we discuss the size limits of the ToolSet.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 2

Web links: `http://www.inria.fr/meije/personnel/madelain/`

Web links: `http://www.inria.fr/meije/meijetools/cost247.evry/slides.html`

Specification of the XTP Context Management Closing Procedure with a TLA

Tatjana Kapus, Zmago Brezocnik

Faculty of Electrical Engineering and Computer Science
University of Maribor
Smetanova ul. 17, SI-2000 Maribor, Slovenia
Email: kapus@uni-mb.si , brezocnik@uni-mb.si
Tel: +386 62 221-112
Fax: +386 62 225-013

We consider the specification of the context management closing procedure of Xpress Transfer Protocol (XTP) in the style of Lamport's Temporal Logic of Actions. It is assumed that a full-duplex association over a pair of lossy channels between two contexts on different hosts is being closed, such that any data for that connection have already been delivered successfully to the hosts. Thus, only the case of the closing procedure is considered where both contexts are active and synchronized initially, and only control messages are needed until the association is closed.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 2

A caching protocol and the Philips Xaccess bus protocol

Susanne Graf

Verimag
Centre Equation
2, avenue de Vignate
F-38610 Gieres
FRANCE

tel : +(33) 4 76 63 48 48
fax : +(33) 4 76 63 48 50
E-mail: Susanne.Graf@imag.fr

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 2

The TIS approach to performance enhancements of LOTOS

A. Wolisz

Technical University Berlin
Institute for Telecommunications
Einsteinufer 25 - D-10587
Berlin Sekr, FT-51
Germany

and

GMD Fokus
Hardenbergplatz 2
D-10623 Berlin
Germany

Tel: 49 30 314 229 11
Fax: 49 30 314 225 14
E-mail: wolisz@ftsu00.ee.tu-berlin.de

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 1-4

Semantics of time constraints in concurrent systems

P. Dembinski

Institute of Computer Science
Polish Academy of Sciences
Ordona 21
PL-01-237 Warsaw
Poland

Tel: 48 22 36284
Fax: 48 22 376564
E-mail: piotrd@wars.ipipan.waw.pl

A truly concurrent and timeless semantics is proposed for a composition (network) of sequential, non-deterministic processes with asynchronous communication. It is shown when this semantics differs from simple interleaving. Implementation-dependent time constraints determine a subset of all computations of the timeless semantics. This subset is precisely characterized for a network of processes and a given set of constraints. It is shown how the same subset may be generated by a timed transition system, i.e., how to simulate a real-time and concurrent system by a non- deterministic and sequential one.

¡P¿ The model for which the above results are obtained, corresponds to that of Estelle with processes being represented by Estelle modules (without nesting). It is more general in that it doesn't limit the communication between modules to port-to-port communication (it allows for arbitrary multicasting) and it doesn't restrict the communication buffers to (infinite) FIFO queues as it is in Estelle.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 4

Performance measures of Estelle specifications

M. Hendaz

Institut National des Telecommunications (INT)
Les Epinettes
9, rue Charles Fourier
91011 EVRY cedex
FRANCE

The traditional approach consisting in using separately FDTs for specification, verification, and validation, and stochastic models for performance evaluation is no longer of great interest in protocols engineering research. A new trend is now growing towards the merging of the two formalisms to provide a complete environment for communication systems development. We present an approach in which performance analysis is conducted on Estelle specifications with annotated quantitative concepts. The potential power of our approach is then demonstrated by an XTP protocol performance analysis.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 4

Web links: `http://alix.int-evry.fr/~stan/edt.html`

Simulation of TIS specifications with practical examples

A. Wolisz

Technical University Berlin
Institute for Telecommunications
Einsteinufer 25 - D-10587
Berlin Sekr, FT-51
Germany

and

GMD Fokus
Hardenbergplatz 2
D-10623 Berlin
Germany

Tel: 49 30 314 229 11
Fax: 49 30 314 225 14
E-mail: wolisz@ftsu00.ee.tu-berlin.de

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 4

Enhancement to LOTOS, status and progression of work

Juan Quemada

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain
Tel: +34 1 3367331
Fax: +34 1 3367333
E-mail: jquemada@dit.upm.es

Overview of the requirements on E-LOTOS and of the different enhancements being considered in the ISO Work Item. This general overview of the status of E-LOTOS may provoke reflections of general nature. The enhaments being considered are:

- Generalized operators. Generalization of termination and enabling to provide an exception handling mechanism and generalization of disabling to provide a suspend/resume operator.

- Event structure. Constructs for typing and tagging gates are considered. The introduction of partial synchronization among events is also considered in the new framework.

- The introduction of time is considered by adding the notion of time passing.

- The introduction of a new data definition part which is executable and which has a rich set of predefined types is considered.

- The introduction of modules is considered.

- The introduction of mobility is considered.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

Web links: `http://www.dit.upm.es/~quemada/`

LotoTis and its Semantics

Ina Schieferdecker

GMD Fokus
Hardenbergplatz 2
D-10623 Berlin
Germany

Tel: +30 254 99 241
Fax: +30 254 99 202
E-mail: ina@fokus.gmd.de

LotoTis is a performance-oriented, upward compatible extension of LOTOS. It is a proposal for enhancing LOTOS with

- *quantified time,*
- *quantified nondeterminism (probabilistic behavior),*
- *quantified parallelism (resources), and*
- *action priorities.*

LotoTis can describe

- *the passage of time in between consecutive events,*
- *the weighted selection among different possible behavior, and*
- *the grade of parallelism within the specification.*

Additionally, LotoTis offers a concept of monitoring that allows us to derive any performance measure of interest from a LotoTis specification.

Structured actions are the central concept of LotoTis. Such a structured action refines the notion of an action in classical process algebras by a set of parameters which can be used to model real-time and other performance-oriented aspects of system tasks. These parameters are the interaction time, the action priority, the set of requested resources, and the monitoring

signal. Structured actions are in general non-instantaneous, may overlap in time, and describe a true concurrent behavior.

It is the use of resources that lead us to a new variant of the classical as soon as possible paradigm: an action must occur as soon as it is enabled and (!) the resources have been allocated. Let us notice that the (unspecified) waiting periods for resources may extend to infinity. Thus, minimal delays are specified by the duration of preceding hidden actions, the duration of actions is modelled by non-zero interaction times, and last but not least, maximal delays are described by the use of timeout operators. It will be shown that LotoTis is equally expressive for the description of time-critical behavior like other time proposals for E-LOTOS. However, we argue that the basic LotoTis assumption of waiting as long as necessary for resources and synchronization partners is the only way to describe quantified parallelism by means of resources.

LotoTis is an upward compatible extension of LOTOS in two respects. Every LOTOS specification is also a LotoTis specification with equivalent semantics. Every LotoTis specification is a refinement of its underlying LOTOS specification. Hence LotoTis supports for the development of performance-oriented specification from existing LOTOS specifications using a number of refinement rules.

After an introduction into LotoTis we will present its semantics. We use the intermediate specification language GENIUS. GENIUS is an upward compatible extension of LOTOS in the sense that it extends LOTOS with additional features while preserving the original LOTOS semantics. GENIUS has an operational semantics. LotoTis is transformed to GENIUS in order to define the LotoTis semantics.

These two steps of semantics definition (from LotoTis to GENIUS, then from GENIUS to SLTS) will be discussed. Afterwards, properties of LotoTis are given.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1-4

Richer Gates for Extended LOTOS

Jose A. Manas

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain

E-mail: pepe@dit.upm.es

Gates in IS LOTOS are simple things to host multi-way rendez-vous. The author proposes several extensions that make gates a powerful and secure structuring object in modular specifications. More precisely, gates will be typed, to avoid discrepancies between declaration and actual use; gates will support tagged arguments, to free argument ordering; and gate types may be in a hierarchy to allow for specification composition from different building sub-specifications. The proposal makes LOTOS usage more secure, and opens a door for reusability of specification components. The talk presents a proposal of the author to the ISO working group on E-LOTOS.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

A Unified Semantical Model for Integration of LOTOS Process and TM Database Specifications, Based on Labelled Transition Systems

Jan J. Vis

University of Twente
INF/IS Po Box 217
7500AE ENSCHEDE
Netherlands

Tel: 31 53 893754
Fax: 31 53 333815
E-mail: Vis@cs.utwente.nl

We aim at developing a formal, declarative specification language, for the design of distributed information systems, by combining the process algebraic language LOTOS for distributed system specification, and the object-oriented data modelling language, and in order to integrate them, their semantical models need to be unified. We examine these two languages, LOTOS and TM and analyze their formal semantics. We define a theoretical framework, in order to unify these semantical models. On the basis of this unified semantics, we discuss a variety of integration aspects of the two languages. We show a wide range of possible approaches to integrate LOTOS and TM specifications, point out their pros and cons, and compare them with respect to expressive power, flexibility, and conceptual clarity.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1-2

Using Functional Data Types in Extended Algebraic Specifications: An Experience Report

Diego Friedel

GMD Fokus
Hardenbergplatz 2
D-10623 Berlin
Germany

Commencing with the drawbacks of the algebraic data type part of standard LOTOS we decided to use functional data types instead. This talk will present our approach of using data types that are written in an Haskell dialect in TIS specification. Example specifications will be given.

Besides a discussion on advantages/disadvantages and experiences with this approach, we show a way of incorporating an existing data type interpreter into our SIMTIS tool. Thus, SIMTIS allows us to simulate full TIS specifications.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

Data Typing for Extended LOTOS

Jose A. Manas

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain

E-mail: pepe@dit.upm.es

Data typing facilities in current LOTOS have been subject to a lot of criticism. There is a strong requirement for E-LOTOS to sort out the problems associated to data in LOTOS and provide something that is usable at industrial scenarios. The presentation will try to focus the problems, and propose solutions, starting with predefined basic data types, basic constructors, syntax and semantics implications. There are a large number of options, so the talk will try to summarize the pros and cons of the most interesting ones, and make a complete, global and coherent proposal. The talk presents a proposal of the author to the ISO working group on E-LOTOS.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

Modules for Extended LOTOS

Jose A. Manas

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain

E-mail: pepe@dit.upm.es

One of the criticism of IS LOTOS is its monolithic nature. There is a single specification text, and at most one standard library. This rigid approach does not permit large groups of specifiers to distribute concerns effectively. A concept of modularity is introduced that aims to remain very simple and abstract, allowing for separate static semantics analysis, via a strict control on name visibility. The concept of modularity allows to distribute assignments after defining an interface, and to check separately the correctness of each piece; it allows for reusability of components, and an smooth evolution throughout the life cycle. The talk presents a proposal of the author to the ISO working group on E-LOTOS.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

The Belgian-Spanish ISO Proposal for a Timed LOTOS

Luc Leonard

Universite de Liege
Systemes et Automatique
Institut Montefiore, bat. B28
B4000 Liege
Belgium
Tel: 32 43 66 49 92
Fax: 32 43 66 29 89
E-mail: leonard@montefiore.ulg.ac.be

At the last ISO/SC21 meeting in Southampton (July 1994), two proposals for a timed extension of LOTOS were submitted, one from Belgium and one from Spain. It was decided to retain the Belgian proposal, with some syntactic features from the Spanish formalism, as basis for further study. Since then, a common proposal has been achieved and submitted to ISO. We will present it, paying a special attention to its semantics.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

On the Algebraic Study of ET-LOTOS

Abdelkader Dekdouk

CRIN-CNRS INRIA Lorraine
BP 239 - F-54506
Vandoeuvre Cedex
France

Tel: +33 3 83 59 20 48
E-mail: dekdouk@lorraine.loria.fr

Our proposal deals with the algebraic study of a temporal extension of Basic LOTOS, and addresses in particular issues related to the definition of strong and weak bisimulation and the collection of equations associated with them. ET-LOTOS represents the basic model, for which we investigate the strong bisimulation and propose some equations to strengthen the collection given by Leduc and Leonard. We also define the observational equivalence which preserves choice, establish the condition for which it is a congruence and characterise this equivalence by a set of equations.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

Timed Modal Specifications: An Extension of CCS with Time and Refinement

Kim Guldstrand Larsen

BRICS
Department of Computer Science
Aalborg University
Fredrik Bajers Vej 7E
DK - 9220 Aalborg
Denmark

Tel: +45 98158522
Fax: +45 98158129
E-mail: kgl@iesd.auc.dk

In this talk the two verification tools TAV and EPSILON will be presented. The presentation will include the formal basis and emphasize the underlying philosophy and pragmatics through applications.

TAV is a tool intended to be useful in constructing CCS (or finite state) implementations in a stepwise refinement and compositional manner. This tool is firmly based on the theory of Modal Specifications allowing loose specifications to be expressed. The theory includes a "bisimulation"-like refinement between specifications and allows specifications to be combined with respect to the operations of CCS.

Recently the theory of Modal Specifications has been extended with explicit real–time constructs. The tool EPSILON provides automatic support for verifying several abstracting refinements between real–time specifications and real–time processes (using Wang Yi's TCCS) as well as model–checking facilities.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1-2

Formal Specification and Generation of Use Cases for a Mobile Telephony Standard

Luigi Logrippo, Amine Rachdi, Randy Tuok

Protocols Research Group
Computer Science Department
University of Ottawa
Ottawa, Ontario
Canada K1N 6N5

Tel: (613)-564-5450
Fax: (613)-564-9486
E-mail: luigi@csi.uottawa.ca

GSM (Global System for Mobile Communications) is a European standard for mobile (cellular) telephony. It was standardized by ETSI (European Telecommunications Standards Institute). It is a digital system which allows international roaming for its subscribers, has sophisticated security features, etc.

LOTOS (Language Of Temporal Ordering Specification) is a formal specification language which is a ISO standard. Its aim is to allow abstract and precise definition of complex distributed systems. Because it is executable, LOTOS specifications constitute a 'model' which can be exercised to see how the entity specified is supposed to work. Because it has formal semantics, LOTOS specifications can be the object of formal validation and verification.

The three main layers of GSM were specified in LOTOS: Radio Resource Management, Mobility Management, and Communications Management. This is the whole of GSM with the exception of the Operation and Management Subsystem. The specification consists of about 3,000 lines of LOTOS. This experience has shown that LOTOS and existing LOTOS tool are well-suited to the task. We present the main philosophy of our speci-

fication approach and the main structural aspects of our specification.The specification can be used to document the standard, to help understand the standard, and as a basis for information exchange between implementors using different platforms.

The main motivation of this exercise was to obtain 'use cases' for GSM. Such use cases are useful in several ways:

- *They can constitute an important documentation aspect of the standard, comparable to time-sequence diagrams.*
- *They can be used for the formal analysis of the specification. For example, by generating appropriate use cases it is possible to see whether security requirements are met.*
- *They can be used for the generation of test cases: in fact, test case generation can be automated to a certain extent by using our specification and appropriate tools.*

In current industrial practice, use cases are generated by hand on the basis of informal specifications. The use of LOTOS and LOTOS methodology simplifies the creation and maintenance of use cases. We describe the methods and tools that were applied to generate automatically GSM use case from the LOTOS specification. Tools used include Ottawa's ELUDO, Grenoble's CAESAR/ALDEBARAN, and Madrid's LOLA.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

Approaches for Detecting Feature Interactions

Luigi Logrippo, Mohammed Faci, and Bernard Stepien

Protocols Research Group
Computer Science Department
University of Ottawa
Ottawa, Ontario
Canada K1N 6N5

Tel: (613)-564-5450
Fax: (613)-564-9486
E-mail: luigi@csi.uottawa.ca

When new functionalities (features) are added to a telephone system, it may be the case that the new features prevent preexisting features from exhibiting their behaviour in the new context, Such design flaws, if not detected at the specification level, may have disastrous consequences once the system is implemented. We present some features for detecting these flaws at the design stage. A telephone system, with its features, is modeled as a collection of communicating oricesses, using LOTOS. In a first approach, LOTOS testing theory is used to detect feature interactions, which show up as deadlocks with appropriately chosen testing processes. In a second approach, feature interactions show up as ambiguities, i.e., cases of non-determinism, which can be detected by a process of backward execution.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 1

The Modeling and Analysis of Frame Synchronized Ring with Predicate/Transition Nets

Tino Pyssysalo

Computer Engineering Laboratory
Department of Electrical Engineering
University of Oulu
P.O. Box 444
FIN-90571 Oulu, Finland

tel: +358-8-553 2701
fax: +358-8-553 2612
E-mail: tino@tks.oulu.fi

The Frame Synchronized Ring (FSR) is a high speed interconnection network (up to 1.6 Gbps and more) developed for a wide range of real-time switching applications in Technical Research Centre of Finalnd (VTT). Examples of such applications are components of Asynchronous Transfer Mode (ATM) networks, high throughput local area networks (LAN) and the distribution of Video on Demand (VOD) services. The high throughput of the FSR is due to an effective distributed medium access control (MAC) mechanism. Some interesting properties of the MAC (e.g. the deadlock freeness, the fairness and maximal worst case waiting sequences) have been extensively analyzed with analytical models and simulations. In this work we use prdecate/transition net formalism (Pr/T-nets) in the modeling and analysis of the FSR. We prove the properties listed above with the Pr/T-net reachability analysis tool, PROD. In addition, we show how the state space of the reachability graph can be reduced by integrating the internal operations of the MAC into as few transitions as possible.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 2

Web links: `http://ee.oulu.fi/~tino`

Verification of the XTP Closing Procedure using a TLA

Tatjana Kapus, Zmago Brezocnik

Faculty of Electrical Engineering and Computer Science
University of Maribor
Smetanova ul. 17, SI-2000 Maribor, Slovenia
Email: kapus@uni-mb.si , brezocnik@uni-mb.si
Tel: +386 62 221-112
Fax: +386 62 225-013

We give a brief presentation of a precise modular design specification of the most important aspects of the closing procedure of the Xpress Transfer Protocol (XTP Protocol Definition, Revision 3.6) written in a temporal logic of actions. We then show how some required safety and liveness properties regarding both graceful and ungraceful closing of XTP data streams can be proved using axioms and special program proof rules of the logic.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 2

Experience with five industrial case studies (Philips1,2,3, NS, Ned.Haarlem, PhilipsH)

Jan Friso Groote

Centrum voor Wiskunde en Informatica
Specification and Analysis of Embedded Systems
P.O. Box 94079
1090 GB Amsterdam
The Netherlands
Email: jfg@cwi.nl
Tel. +31-20-5924232
Fax. +31-20-5924199

We report on five case studies that we have caried out during the last years with Dutch industries. These concern the specification of consumer electronics (2x) as well as the verification of these (1x). Reverse engineering of switching units (1x), proving safety of railway control (1x) and specifying the behaviour of traffic lights. The general conclusion is that in all cases our work did exceptional well, in the sense that with relative ease we could clarify and understand the systems under consideration. Another conclusion is that the current culture in most industries is such that although the contributions of our work are acknowledged, it is not easy to make formal methods part of daily industrial design.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 2

Web links: `http://www.cwi.nl/~jfg`

Design and use of Estelle/SDL enhanced simulators for performance predictions of a prototype XTP protocol implementation

Stanislas Budkowski

Institut National des Telecommunications (INT)
Les Epinettes
9, rue Charles Fourier
91011 EVRY cedex
FRANCE
Tel: +33 1 60 76 47 20
Fax: +33 1 60 78 39 27
E-mail: stan@int-evry.fr

The Edb simulator (a part of the EDT (Estelle Development Toolset) package)) and SPEC tool both having fonctions allowing collection of performance evaluation measures will be briefly presented. The Edb simulator performs measures on Estelle specifications while SPEC tool on SDL specifications.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 4

Web links: `http://alix.int-evry.fr/~stan/edt.html`

Simulating Extended Algebraic Specifications with SES Workbench: the SIMTIS Approach

Jean-Pierre Ebert and Morten Schlaeger

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 4

An implementation of SDL 92 synchronization semantics

Vladimir Levin, Husnu Yenigun and Kemal Inan

Electrical & Electronics Engineering Department
Middle East Technical University
Ankara 06531, Turkey
e-mail : inan@srdc.metu.edu.tr
tel : +90-312-2101298 and +90-312-2102324
fax : +90-312-2101411 and +90-312-2101261

SDL semantics has nontrivial communication semantics in which target addressing and process spawning necessitates conceptualization of a communication network that matches the semantical requirements of SDL in implementation. We present the features of this underlying communication semantics.

This presentation has been given during the COST-247 4th Management Committee Meeting (Berlin, Germany, February 9–10, 1995).

COST-247 Working Group(s): 4

Open Distributed Processing: new challenges for Formal Methods

Maarten Steen, Eerke Boiten, Howard Bowman and John Derrick

Computing Lab.
University of Kent at Canterbury
Kent CT2 7NF
United Kingdom
Email: mwas@ukc.ac.uk
Tel: +44 1227 764000 x3822
Fax: +44 1227 762811

This presentation will give an overview of the Reference Model for Open Distributed Processing and the challenges it presents to the formal methods community.

The RM-ODP is a natural progression from the OSI Reference Model, extending the scope of standardisation from the point of interconnection to the end-to-end system behaviour. The objective is to enable the construction of distributed systems in a multi-vendor environment through the provision of a general architectural framework that such systems must conform to.

One of the cornerstones of this framework is a model of multiple viewpoints, each with an associated viewpoint language. The five ODP viewpoints (enterprise, information, computational, engineering and technical) provide a set of models each aimed at capturing one facet of the design. Requirements and specifications of an ODP system can be made from any of these viewpoints. This is in contrast with the traditional waterfall model that most formal design methodologies adhere to.

The following challenges can be identified:

- *Definition of architectural semantics for ODP i.e., finding appropriate interpretations of the viewpoint language concepts in existing FDTs.*
- *Conformance testing methods that test for the end-to-end behaviour.*

- *Provision of consistency checking techniques in order to determine whether the multiple specifications impose conflicting requirements.*
- *Translation between different formalisms in order to relate the viewpoint specifications.*

This presentation has been given during the COST-247 5th Management Committee Meeting (Warsaw, Poland, June 12–13, 1995).

COST-247 Working Group(s): 1

Web links:
`http://alethea.ukc.ac.uk/Dept/Computing/Research/NDS/consistency/`

Transformation of ET-LOTOS Processes in Extended Timed Automata

Christian Hernalsteen

Universite Libre de Bruxelles
Departement d'Informatique, CP212
Bl. du Triomphe
Brussels, Belgium
e-mail: chernals@ulb.ac.be
tel: +32 2 650 50 42
fax: +32 2 650 56 09

We propose to define a framework to verify TCTL formulas on ET-LOTOS specification. The first step is to define an extended timed automaton in which ET-LOTOS will be transformed. This intermediate representation will be more easy to handle for the verification of TCTL formulas. The timed automaton is extended with variables. The transformation of all the ET-LOTOS operators (except the generalized choice) has been defined including the process instantiation. The idea is to develop a method to verify TCTL formulas on this extended timed automaton. This part will be undertaken in a near future.

This presentation has been given during the COST-247 5th Management Committee Meeting (Warsaw, Poland, June 12–13, 1995).

COST-247 Working Group(s): 1

A refinement technique in SDL design of a telephone exchange

Eleonora Bounimova, Vladimir Levin, Kemal Inan

Electrical & Electronics Engineering Department
Middle East Technical University
Ankara 06531, Turkey
e-mail : inan@srdc.metu.edu.tr
tel : +90-312-2101298 and +90-312-2102324
fax : +90-312-2101411 and +90-312-2101261

SDL description of a small scale PABX is described and a method for the refinement of the specification is suggested in which the size of the state space is reduced by exploiting certain properties.

This presentation has been given during the COST-247 5th Management Committee Meeting (Warsaw, Poland, June 12–13, 1995).

COST-247 Working Group(s): 4

Insyde - An Integrated methodology for Hybrid System Design

Eckhardt Holz

Humbolt University
Lindenstr. 54 a
D-10099 Berlin
Germany

Tel: 49 30 20181241
Fax: 49 30 20181234
E-mail: holz@informatik.hu-berlin.de

This presentation has been given during the COST-247 5th Management Committee Meeting (Warsaw, Poland, June 12–13, 1995).

COST-247 Working Group(s): 4

phi-SDL as the core of SDL with a tractable semantics

Kees Middelburg

Department of Philosophy
Utrecht University
P.O.Box 80126
3508 TC Utrecht
Netherlands
Tel: +31 30 253 55 79
Fax: +31 30 253 28 16
E-mail: Kees.Middelburg@phil.ruu.nl

A new semantics of an interesting subset of the specification language SDL is given by a translation to a discrete-time extension of process algebra in the form of ACP extended with data added as in muCRL. The strength of the chosen subset, called phiSDL, is its close connection with full SDL, despite its dramatically reduced size. Thus, we are able to concentrate on solving the basic semantic issues without being in danger of having to turn the results inside out in order to deal with full SDL. Novel to the presented semantics is that it relates the time used with timer setting to the time involved in waiting for signals and delay of signals.

This presentation has been given during the COST-247 5th Management Committee Meeting (Warsaw, Poland, June 12–13, 1995).

COST-247 Working Group(s): 4

Web links: `http://www.phil.ruu.nl/home/keesm/uireport68.ps`

Web links: `http://www.phil.ruu.nl/home/keesm/`

COST-247 Working Group(s): 4

Features of a new process algebra

Kemal Inan

Electrical & Electronics Engineering Department
Middle East Technical University
Ankara 06531, Turkey
e-mail : inan@srdc.metu.edu.tr
tel : +90-312-2101298 and +90-312-2102324
fax : +90-312-2101411 and +90-312-2101261

A new process algebra is presented in which the synchronization scope can dynamically change. This flexibility of synchronization has advantages of simplicity in expression as demonstrated via a few examples.

This presentation has been given during the COST-247 5th Management Committee Meeting (Warsaw, Poland, June 12–13, 1995).

COST-247 Working Group(s): 1

Specification Architecture in a Communications Context

Kenneth J. Turner

Department of Computing Science and Mathematics
University of Stirling
Stirling FK9 4LA
United Kingdom
Email: kjt@cs.stir.ac.uk
Tel: +44 1786 832 602
Fax: +44 1786 467 420

The concept of specification architecture is introduced, and its importance is emphasised. Three important architectural principles are offered as a way of achieving a satisfactory specification architecture: modularity, generality and simplicity. These are supported by subsidiary techniques that realise them. Criteria are identified to evaluate successful application of the techniques and conformance to the principles. The approach is illustrated throughout with the example of a message switch, culminating in a larger case study based on the work of the PANGLOSS project to design a high-speed message switch.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 1

Web links: `http://www.cs.stir.ac.uk/~kjt/research/`

Focus Points and Convergent Process Operators

Jan Friso Groote

Centrum voor Wiskunde en Informatica
Specification and Analysis of Embedded Systems
P.O. Box 94079
1090 GB Amsterdam
The Netherlands
Email: jfg@cwi.nl
Tel. +31-20-5924232
Fax. +31-20-5924199

We are searching for improved ways to prove the correctness of distributed systems and protocols. Our investigation has led to a method that we baptise the Cones and Foci method. A parallel process is first transformed in a linear process by expanding the parallellism. By using convergent process operators, the description remains relatively small and the state space explosion is circumvented. Then, in order to prove a specification equal to an implementation, six sets of requirements need to be checked. Using this method we have proven a number of rather intricate distributed systems correct.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 1

Web links: `http://www.cwi.nl/~jfg`

An overview of the LOTOSPHERE proposal for modules in E-LOTOS

Hubert Garavel and Mihaela Sighireanu

INRIA Rhone-Alpes / Dyade
655, avenue de l'Europe
38330 MONTBONNOT ST MARTIN
FRANCE
tel: +(33) 4 76 61 52 24
fax: +(33) 4 76 61 52 52
E-mail: hubert.garavel@inria.fr

Because modules are a desirable feature for programming-in-the-large, there is a requirement for introducing modules in the future E-LOTOS (Enhanced Lotos) standard. We present here the salient features of a proposal for a simple, algebraic system of modules on top of LOTOS, which has been developed in the ESPRIT LOTOSPHERE project.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 1

Web links: `http://www.inrialpes.fr/vasy`

Formal specification and implementation of an SDL to COSPAN compiler

Kemal Inan

Electrical & Electronics Engineering Department
Middle East Technical University
Ankara 06531, Turkey
e-mail : inan@srdc.metu.edu.tr
tel : +90-312-2101298 and +90-312-2102324
fax : +90-312-2101411 and +90-312-2101261

The features of a compiler from the language SDL into the language S/R is described. The latter is the input language of a verification tool COSPAN, both developed at AT&T. The purpose of the compiler implementation exercise was to use the verification tool COSPAN for SDL programs. An additional feature of COSPAN is a timing module in which it is possible to verify concurrent software with hard real time constraints.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 1

A first experiment with ET-LOTOS: The specification of real-time schedulers

Christian Hernalsteen

Universite Libre de Bruxelles
Departement d'Informatique, CP212
Bl. du Triomphe
Brussels, Belgium
e-mail: chernals@ulb.ac.be
tel: +32 2 650 50 42
fax: +32 2 650 56 09

Three different real-time schedulers have been specified using the formal description language ET-LOTOS. The first one handles independent periodic tasks characterized by their period, execution time and deadline. The scheduler is cyclic; it considers the system every "delta" time units. The second one handles the same kind of tasks but in an event driven way. The scheduler is woken up by two kinds of events: the begining of a new task occurence and the end of the current executing task. The last scheduler is also event-driven but considers dependent tasks. The scheduled tasks are represented by a sequence of independent execution-time and interaction points which are represented by semaphores. These three schedulers are preemptive and schedule tasks based on a static priority policy. Problems of deadlocks and priority inversion are not resolved in these schedulers.

For each of these schedulers, an ET-LOTOS specification is given for the scheduler and for the tasks. The tasks must be defined since they interact with the scheduler for the CPU allocation. A task can be in one of the following states: running, preempted or waiting for its next occurence. Each of these states is represented by an ET-LOTOS process. The specification has been done in a stepwise way, where a prelimary description is done and then modified several times to resolve some apparent timing problems. These different specification steps are presented in the paper in order to show what kind of problems the specifier must be aware of when

using a timed specification description language like ET-LOTOS. Indeed some new problems can arise with this language that never occur with non timed specification languages.

The produced specifications are not very large but use all the ET-LOTOS operators and give a good intuition of the expressive power of the language.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 1

Reduction Method for Transition System of a Performance Evaluation Extension of LOTOS

Z. Huzar(1) and J. Magott(2)

Computer Science Department

Technical University of Wroceaw, Poland
Tel: (48) (71) 3203431
Fax: (48) (71) 211018

(2) Institute of Engineering Cybernetics
Faculty of Electronics,
Technical University of Wroceaw, Poland

E-mail: z.huzar@ci.pwr.wroc.pl , magott@ict.pwr.wroc.pl

The proposal presents extensions of specification language LOTOS in two directions: time consuming actions and performance evaluation constructions. Time consuming actions often seem to be more natural than instantaneous actions and they are well suited for real-time system specification and for its performance evaluation. The notions of beginning and termination of the time consuming action enable to impose time restrictions on beginning and termination times of activities. From performance evaluation point of view it is often important to know explicit how long a specific action has been executed (not when the action has been completed only). We have defined such a performance evaluation extension of LOTOS that can be used as a modelling language for performance evaluation of distributed systems. A semantics that expresses overlapping of time consuming actions in time is defined. A reduced transition system for the extension is defined. This reduction when comparing with original transition system has two advantages. First, the reduced transition system contains aggregated transitions that are a result of appearing many events in the same time instant. Second, this reduction eliminates some states. The reduction is essential

for transition systems with actions of two scales of execution time: short and long actions. The greater the ratio of short actions to long actions is the greater the reduction of the number of states of the transition system is. By means of the reduced transition system we express the true concurrence semantics of our language. Our extension towards performance evaluation can be used as a basis for both simulation and analytic approaches.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 1-4

Conformance test results in Hungary

Endre Blum and Cs.Elekes and Andras Bolcskei

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 3

Certification in Hungary

Janos Miskolczi and Kati Tarnay

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 3

Derivation of protocols for specific users of distributed systems

Marjeta Pucko and Monika Kapus-Kolar

Jozef Stefan Institute
Digital communications and networks department
POB 3000, SI-1001 Ljubljana, Slovenia

Tel: +386 61 1773 724
Fax: +386 61 1262 102
E-mail: marjeta.pucko@ijs.si , monika.kapus-kolar@ijs.si

A family of algorithms for automated protocol derivation using service-driven protocol synthesis has been developed in the last four years at the Jozef Stefan Institute, Ljubljana, Slovenia. Much work has recently been done on protocol synthesis for specific users. We propose some improvements of earlier protocol synthesis methods that give to a specific user of a distributed system service the possibility to generate a more efficient and correct protocol. Optimization of the derived protocol is achieved by considering eventual redundancies in the service specification and the actual testing capabilities of the particular service user.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 3, 1

Specification of abstract test suites in MSC

Maria Toeroe

KFKI Research Institute for Measurement and Computing Techniques
H-1525 Budapest, P.O.Box 49, Hungary

Tel: 36 1 395 9220
Fax: 36 1 395 9027
E-mail: tmaria@sun60.mszki.kfki.hu1

In a protocol life cycle different standard FDTs may be used. To avoid alteration in languages usually applied MSC has been investigated to determine whether it can be used to specify abstract test suites. The stressed point of this investigation is the possibility to define alternative behaviours in MSC. It is demonstrated that rules of composition/decomposition allow one to specify alternative behaviour, however, not by one, but by a set of message sequence charts. The relationship of these charts may be shown on a functional decomposition diagram suggested by the SDL Methodology Guidelines of Z.100 Recommendation.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 3

Specification in LOTOS and verification of a distributed election algorithm

Hubert Garavel and Laurent Mounier

INRIA Rhone-Alpes / Dyade
655, avenue de l'Europe
38330 MONTBONNOT ST MARTIN
FRANCE
tel: +(33) 4 76 61 52 24
fax: +(33) 4 76 61 52 52
E-mail: hubert.garavel@inria.fr

This talk deals with the formal specification and verification of distributed leader election algorithms for a set of machines connected by a unidirectional ring network.

Starting from an algorithm proposed by Le Lann in 1977, and its variant proposed by Chang and Roberts in 1979, we study the robustness of this class of algorithms in presence of unreliable communication medium and/or unreliable machines. We suggest various improvements of these algorithms in order to obtain a fully fault-tolerant protocol.

These algorithms are formally described using the ISO specification language LOTOS and verified (for a fixed number of machines) using the CADP (CAESAR/ALDEBARAN) toolbox. Model-checking and bisimulation techniques allow the verification of these non-trivial algorithms to be carried out automatically.

This presentation has been given during the COST-247 6th Management Committee Meeting (Budapest, Hungary, October 26-27, 1995).

COST-247 Working Group(s): 1-2

Web links: `http://www.inrialpes.fr/vasy`

A process-algebraic approach to compute and represent the global events of a LOTOS specification preserving parallelism

David Larrabeiti Lopez

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain

E-mail: dlarra@dit.upm.es

The approach followed in this work broaches the state explosion problem within the LOTOS framework, through the development of a representation method and a compact state space exploration algorithm based on it, with several applications. The model proposed allows a compact representation of parallelism, reducing the impact of the interleaving semantics of LOTOS in the state explosion. The algorithm that converts any LOTOS expression into an equivalent expression in the new calculus is called interleaved expansion. The interleaved expansion yields a representation of the labeled transition system where interleaving behaviours are isolated, factored and kept unexpanded. This representation implies an important size reduction with respect to the explicit transition system in those specification with a high degree of interleaving. Hence it is suitable for specifications written in a resource-oriented style. On the other hand, the size of the interleaved expanded form can be bigger than its equivalent transition system in certain cases of specifications written following a constraint-oriented approach. In practice, this is not a major disadvantage, since state explosion appears mainly in resource-oriented specifications. Furthermore, a normal expansion can be applied in such cases.

The development presented contains the extension of the model to full LOTOS and a comparison with some related true concurrency semantics models, such as Petri nets and event structures. Finally, the study includes

an algorithm for state exploration which preserves interleaving zones and which is compatible with reduction methods based on stubborn sets principles.

The implementation of the interleaved expansion has allowed to check the results on medium sized sample specifications.

This work has been partially supported by SIGMA and MEDAS projects (finished).

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 1

State Exploration in TE-LOTOS with Time Extended LOLA

Gualberto Rabay Filho

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain

Tel: +34 1 5495700 Ext 442
Fax: +34 1 3367333
E-mail: grabay@dit.upm.es

TE-LOLA (Timed Extended Lotos LAboratory) is a software prototype that supports full TE-LOTOS according to the current ISO working group proposal. TE-LOLA's functionality includes: Expansion (EFSM generation), Parameterized Expansion, Interleaved Expansion, Timed Testing and Timed Simulation/Debugging. This presentation explains relevant issues regarding state exploration in TE-LOTOS.

The analysis of timed LOTOS specifications is more complex than the untimed one for many reasons. First, it is necessary to carry out extra functions (intersection of time intervals of participating actions in synchronizations, implementation of aging, urgency action pruning, etc..). Second, the generated state space is almost always much bigger due to the generation of time variables in the aging process, even considering elimination of states that violate time constraints. And third, interval time constraints induce a heavy and complicated symbolic computation not easy to deal with formally.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 1

Web links: `http://www.dit.upm.es/~grabay/`

Hardware Implementation of LOTOS specifications

Tomas de Miguel, Tomas Robles Valladares

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain

E-mail: robles@dit.upm.es

Our group has developed a compiler from LOTOS to VHDL. Such compiler performs translation of behaviour, data types and time annotations. Translation may be done with three targets: simulation, implementation or testing.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 1

EMPA : A Stochastic Process Algebra

Marco Bernardo

Universita' di Bologna
Dipartimento di Scienze dell'Informazione
Mura Anteo Zamboni 7
40127 Bologna
Italy
E-mail: bernardo@cs.unibo.it
Tel: +39 51 354516
Fax: +39 51 354510

An integrated approach for modeling and analyzing functional and performance properties of concurrent systems is proposed, which is based on Extended Markovian Process Algebra (EMPA) and Generalized Stochastic Petri Nets (GSPNs). EMPA is a process algebra where each action is a pair composed of the type, which expresses the functionality of the action, and the rate, which expresses the duration of the action. EMPA is introduced together with its integrated interleaving semantics (a transition system labeled on both action types and action rates), its functional semantics (a transition system labeled on action types only), its performance semantics (a homogeneous continuous-time Markov chain), and its integrated truly concurrent semantics (a GSPN). Finally, the case study of the alternating bit protocol is presented in order to illustrate the integrated approach as well as the expressive power of EMPA.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 1-4

Web links: `http://www.cs.unibo.it/~bernardo`

Implementation relations for Transition System Specifications

Jan Tretmans

Tele-Informatics and Open Systems Group
Department of Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede, The Netherlands
email: tretmans@cs.utwente.nl
tel: +31 53 489 4287
fax: +31 53 489 3247

Implementation relations, formalizing the notion of correctness of implementations with respect to specifications, are presented for labelled transition systems. Starting from the well-known principles of testing equivalence and refusal testing for transition systems, analogous ideas are applied to transition systems in which the actions can be partitioned into inputs and outputs, and where inputs are always enabled. This leads to a simplification of the testing theory. The relations with the theories of Input/Output Automata and Input-Output State Machines is indicated.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 1

An overview of the EUCALYPTUS project

Hubert Garavel

INRIA Rhone-Alpes / Dyade
655, avenue de l'Europe
38330 MONTBONNOT ST MARTIN
FRANCE
tel: +(33) 4 76 61 52 24
fax: +(33) 4 76 61 52 52
E-mail: hubert.garavel@inria.fr

This article presents the essential features of a protocol engineering environment, the EUCALYPTUS toolbox, which has been developed or improved in the framework of two successive European-Canadian projects EUCALYPTUS-1 and EUCALYPTUS-2. This toolbox is based on the formal description technique LOTOS standardized by ISO. It offers a wide range of functionalities, including simulation, compilation, verification and test case generation for LOTOS descriptions.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 1-2

Web links: `http://www.inrialpes.fr/vasy`

SPEC: SDL Performance Evaluation Tool

Stan Budkowski

Institut National des Telecommunications (INT)
Les Epinettes
9, rue Charles Fourier
91011 EVRY cedex
FRANCE
Tel: +33 1 60 76 47 20
Fax: +33 1 60 78 39 27
E-mail: stan@int-evry.fr

This talk shortly presents a software tool developed at the University of Cape Town (South Africa).

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 4

Performance Estimations based on an XTP Formal Specification

Piotr Dembinski

Institute of Computer Science
Polish Academy of Sciences
Ordona 21
PL-01-237 Warsaw
Poland

Tel: 48 22 36284
Fax: 48 22 376564
E-mail: piotrd@wars.ipipan.waw.pl

The talk describes the work in progress within Workpackage 2 "analysis of properties of protocols for high speed networks supporting multimedia applications" of the project COPERNICUS 62. The part that is addressed in this talk concerns the problem of incorpating into the protocol development process some early performance estimations of an implied protocol implementation.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 4

Specification and Implementation of Components of a Toolbox for muCRL

Jan Friso Groote

Centrum voor Wiskunde en Informatica
Specification and Analysis of Embedded Systems
P.O. Box 94079
1090 GB Amsterdam
The Netherlands
Email: jfg@cwi.nl
Tel. +31-20-5924232
Fax. +31-20-5924199

Using the toolbus we have developed a set of tools to build toolsets for muCRL. In order to use our own methodology we have first specified the required behaviour of the tools as well as an implementation in muCRL. In principle this would allow to prove the correctness of the implementations. Then, the tools have been realized using C. Our conclusion is that the design of the systems in muCRL was the major part of the work, but led to very concise and intelligible descriptions. Implementation in C was for the major part a straightforward activity.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 1

Web links: `http://www.cwi.nl/~jfg`

Optimal Checking Sequence Construction Under Differing Set of Assumptions Exploiting Overlapping Constraints

Kemal Inan

Electrical & Electronics Engineering Department
Middle East Technical University
Ankara 06531, Turkey
e-mail : inan@srdc.metu.edu.tr
tel : +90-312-2101298 and +90-312-2102324
fax : +90-312-2101411 and +90-312-2101261

Theory of exhaustive checking sequence generation is presented in which problems of optimality are formulated and solved in terms of synthesis of a path with patch constraints on an I/O automaton.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 3

A logic and compositional proof system for Erlang: An overview

Fredrik Orava

KTH/Teleinformatik
Electrum 204
S-164 40 KISTA
SWEDEN

Tel: +46 8 752 1490
Fax: +46 8 751 1793
E-mail: fredrik@it.kth.se

In this talk we describe ongoing work on developing a compositional proof system for the concurrent functional programming language Erlang. Three main components of the work are: a (Plotkin-style) operational semantics for a core fragment of Erlang including recursion, parallelism, communication and process spawning; a specification logic for the Erlang fragment based on the modal mu-calculus; and a compositional proof system for establishing that Erlang programs possesses properties expressed in the specification logic. The proof system is based on an early prototype tool for the pi-calculus developed at SICS. An early implementation of the system can be demonstrated on request.

This presentation has been given during the COST-247 7th Management Committee Meeting (Madrid, Spain, February, 12–13, 1996).

COST-247 Working Group(s): 2

Commercial Verification

Robert Kurshan

AT&T Bell Labs
Murray Hills
New Jersey
USA

Recently, increasing complexity of hardware designs and theoretical breakthroughs in algorithmic verification have provided the opportunity for formal verification to emerge from academia to commerce. Suddenly, there are at least four serious design tools based upon the theory of formal verification, available in the commercial market, with more on the way. I will discuss the basis and future of this new trend.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 2

SOFTWARE/HARDWARE CO-DESIGN USING THE TWO SPECIFICATION LANGUAGES: SDL AND S/R

Ella Bounimova

TUBITAK Software R&D Center
METU Computer
Engineering Department
Ankara
Turkey

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s):

OBJECT ORIENTED MODELLING OF ADVANCED IN SERVICES WITH SDL-92

Ferdinando Lucidi, Alessandro Tosti, Sebastiano Trigila

Fondazione Ugo Bordoni
Telecommunication Networks Department
via Baldassarre Castiglione 59
00142 Roma Italy
Email: nando@fub.it
Tel: +39 6 5480 3342
Fax: +39 6 5480 4404

Long term trends in a telecommunication market characterizaded by a fast evolving technology, a multiplicity of providers and the presence of chains of value-added services, call for architectural frameworks which allow the introduction of new and enhanced services and their management, much faster and more efficiently than possible today. The Intelligent Network (IN) standards [Q.12xx] have been defined to meet this demand taking as a starting point the basic telephony system architectures.

This paper describes a methodology for specification, validation and implementation of IN services and service features based on SDL-92 and its object-oriented constructs [Z.100]. This methodology has been exercised in the realm of the Universal Personal Telecommunication service.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 4

EXPERIENCE OF USING SDL IN ISKRATEL

Ana Robnik

ISKRATEL
Ljubljanska c. 24a, SI-4000 Kranj, Slovenia
Email: robnik@iskratel.si
Tel: +386 64 272-686
Fax: +386 64 221-525

This paper summarises the experience of introducing SDL and MSC and also reflects recent and future work in the ISKRATEL company. ISKRATEL SDL Methodology (ISDLM) and prototype development CASE Study are briefly reviewed here. The extended and added features during the design, simulation and implementation phases are described in detail. The final results of the prototype and products development are being discussed here. Finally, the experience of using SDL-88 and the GEODE tool is mentioned, as are our future plans and expectations.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 4

Specifying and verifying the alternating bit protocol with probabilistic-timed LOTOS

Carlos Gregorio-Rodriguez and Manuel Nunez

Dept. de Informatica y Automatica
Universidad Complutense de Madrid
E-28040 Madrid, Spain
E-mail: cgregor@dia.ucm.es , manuelnu@dia.ucm.es

In this paper we use a probabilistic-timed version of Lotos (PTLotos) for specifying and verifying the Alternating Bit Protocol (ABP). First, we present the language which is an upward compatible version of Lotos where some new operators to deal with time and probabilistic features have been included. We give an operational semantics, where there are two kinds of transitions: probabilistic transitions and timed transitions. Transitions of the first kind are associated with the events that a behavior expression can execute, while timed transitions deal with time evolution. From this operational semantics we define a testing semantics, where a process passes a test with a probability in a period of time, and two processes are intended to be equivalent if they pass all the tests with the same probability for any time.

In the second part of the paper, we use PTLotos in order to specify the Alternating Bit Protocol. The ABP is a simple communication protocol which provides an error free communication over a faulty medium. The protocol has three components: the sender, the receiver and the (faulty) medium, where we suppose that the medium may lose the messages. The only observable events of the whole system will be mess (indicating that a message has been sent) and deli (indicating that a message has been received and delivered). Once we have specified the three components and we have described the whole system, we verify that our specification fulfills some good properties. Because of the testing semantics we have defined, we can make assumptions about the environment, and we can express them using tests, and so, we can get information about the behavior of the protocol

by studying the interaction between such tests and the specification of the ABP.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 1-2

AN EXPERIMENT IN FORMALISING AND ANALYSING RAILYARD CONFIGURATIONS

Lars-ake Fredlund and Fredrik Orava

KTH/Teleinformatik
Electrum 204
S-164 40 KISTA
SWEDEN

Tel: +46 8 752 1490
Fax: +46 751 1793
E-mail: fredrik@it.kth.se , fred@sics.se

We present a method by which the abstract behaviour of railyards can be specified, and analysed for safety. Our analysis is based on well established railway signalling concepts such as train routes *and* flank protection *and attempts to verify safety properties which state that if the railyard is configured in a correct way, no unwanted situations such as train collisions or derailings will occur. We specify the railyards in process algebra and the safety properties in the modal μ-calculus.*

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 1-2

Functionality decomposition of basic Lotos expressions with generalized termination, enabling and disabling

Monika Kapus-Kolar

Jozef Stefan Institute
Digital communications and networks department
POB 3000, SI-1001 Ljubljana, Slovenia

Tel: +386 61 1773 531
Fax: +386 61 1262 102
E-mail: monika.kapus-kolar@ijs.si

A correctness-preserving transformation is proposed for functionality decomposition of Basic LOTOS expressions with generalised termination, enabling and disabling. Given a specification of the required external behaviour, i.e. the expected service of a distributed system, and a partitioning of the specified actions among the system components, the transformation derives behaviour of individual system components implementing the service. There may be an arbitrary finite number of system components pairwise communicating over auxiliary LOTOS gates.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 1

Demonstration of the CAESAR/ALDEBARAN toolbox

Hubert Garavel

INRIA Rhone-Alpes / Dyade
655, avenue de l'Europe
38330 MONTBONNOT ST MARTIN
FRANCE
tel: +(33) 4 76 61 52 24
fax: +(33) 4 76 61 52 52
E-mail: hubert.garavel@inria.fr

CADP (CAESAR/ALDEBARAN Development Package) is a toolbox for protocol engineering. It offers a wide range of functionalities, from interactive simulation to the most recent formal verification techniques. CADP is jointly developped by the VASY action at INRIA Rhone-Alpes / DYADE and the Verimag laboratory. It is dedicated to the efficient compilation, simulation, formal verification, and testing of descriptions written in the ISO language LOTOS [ISO standard 8807].

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 1-2

Web links: `http://www.inrialpes.fr/vasy`

TE-LOLA: A Time Extended LOLA prototype

David Larrabeiti, Gualberto Rabay Filho

Dept. Ingenieria de Sistemas Telematicos
Universidad Politecnica de Madrid
ETSI Telecomunicacion
E-28040 Madrid
Spain

Tel: +34 1 5495700 Ext 375 (Larrabeiti) Ext 442 (Rabay)
fax: +34 1 3367333
E-mail: dlarra@dit.upm.es , grabay@dit.upm.es

TE-LOTOS (Time Extended LOTOS) is the current ISO proposal for extending Standard LOTOS with quantitative time. Real time features were introduced by defining timed events which should happens in concrete instants of time. LOLA (LOTOS LAboratory) is a Full Standard LOTOS exploration and analysis tool which is one of the components of the DIT/UPM LOTOS Tool Set TOPO. TE-LOLA is a LOLA-based prototype that supports TE-LOTOS. The current version runs on SunOS 4.1.3 and Solaris 2.3 but portability to other platforms is straightforward. TE-LOLA has almost the same functionality as LOLA, supporting the following transformations: Expansion (EFSM generation), Parameterized Expansion, Interleaved Expansion, Timed Testing and Timed Simulation/Debugging.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 1-2

Web links: `http://www.dit.upm.es/~dlarra/`

Web links: `http://www.dit.upm.es/~grabay/`

FORMAL DESCRIPTION AND ANALYSIS OF A BOUNDED RETRANSMISSION PROTOCOL

Radu Mateescu

INRIA Rhone-Alpes / Dyade
655, avenue de l'Europe
38330 MONTBONNOT ST MARTIN
FRANCE
tel: +(33) 4 76 61 52 83
fax: +(33) 4 76 61 52 52
E-mail: radu.mateescu@inria.fr

This talk reports about the formal specification and verification of a Bounded Retransmission Protocol (BRP) used by Philips in one of its products. We started with the descriptions of the BRP service (i.e., external behaviour) and protocol written in the mCRL language by Groote and van de Pol. After translating them in the LOTOS language, we performed verifications by model-checking using the CADP (CAESAR/ALDEBARAN) toolbox. The models of the LOTOS descriptions were generated using the CAESAR compiler (by putting bounds on the data domains) and checked to be branching equivalent using the ALDEBARAN tool. Alternately, we formulated in the ACTL temporal logic a set of safety and liveness properties for the BRP protocol and checked them on the corresponding model using our XTL generic model-checker.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 1-2

MODELLING AND VERIFYING A BOUNDED RETRANSMISSION PROTOCOL USING UPPAAL

Pedro R. D'Argenio, Joost-Pieter Katoen, Theo Ruys, and Jan Tretmans

Tele-Informatics and Open Systems Group
Department of Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede, The Netherlands
E-mail: tretmans@cs.utwente.nl , dargenio@cs.utwente.nl ,
katoen@cs.utwente.nl , ruys@cs.utwente.nl
tel: +31 53 489 4287
fax: +31 53 489 3247

This paper concerns the transfer of files via a lossy communication channel. It formally specifies this file transfer service in a property-oriented way and investigates—using two different techniques—whether a given bounded retransmission protocol conforms to this service. This protocol is based on the well-known alternating bit protocol but allows for a bounded number of retransmission of a frame, i.e., part of a file, only. So, eventual delivery is not guaranteed and the protocol may abort the file transfer. We investigate to what extent real-time aspects are important to guarantee the protocol's correctness and use SPIN *and* UPPAAL *model checking for our purpose. A comparison between these approaches is made and our experiences are reported.*

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 2

ANALYSIS OF COMMUNICATION PROTOCOLS USING A THEORY OF LOSSY CHANNEL SYSTEMS

Parosh Aziz Abdulla

Department of Computer Systems
University of Uppsala
Box 325
S-751 05 Uppsala
SWEDEN

E-mail: parosh@docs.uu.se

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 2

ABRUPTLY-TERMINATED CONNECTIONS IN TCP – A VERIFICATION EXAMPLE

Ina Schieferdecker

GMD Fokus
Hardenbergplatz 2
D-10623 Berlin
Germany
Tel: (030) 254 99 241
Fax: (030) 254 99 202
e-mail: ina@fokus.gmd.de

The talk presented the verification of a functional misbehavior in TCP, that is one of the widely used transport protocols used in the Internet. The solution that was developed by I. Heavens is verified for its correctness. A model checking approach is used to verify TCP: the protocol is described in LOTOS and the requirements are given in the modal μ-calculus. The verification uses the CADP tool set for automating the verification process.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 1-2

EFFICIENT SYMBOLIC TRAVERSAL ALGORITHMS USING PARTITIONED TRANSITION RELATIONS

Zmago Brezocnik, Ales Casar, Tatjana Kapus

Faculty of Electrical Engineering and Computer Science
University of Maribor
Smetanova ul. 17, SI-2000 Maribor, Slovenia
Email: brezocnik@uni-mb.si , casar@uni-mb.si , kapus@uni-mb.si
Tel: +386 62 221-112
Fax: +386 62 225-013

This paper presents an efficient tool for symbolic state space traversal of finite state machines. Both algorithms for searching reachable states and for model checking in CTL owe their efficiency primarily to an improved state variables substitution algorithm and to the use of partitioned transition relations. Partitioning of the relations is fully automatic. We give experimental results on the performance of the algorithms applied to a set of synchronous benchmark circuits.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 2

Verification of Signalling Protocols for Telecommunication Services in Intelligent Network

Bruno Blaskovic, Ignac Lovrek

University of Zagreb
Faculty of Electical Engineering and Computing
Unska 3
HR-10000 Zagreb
Croatia

Tel: +385 1 612 98 02
Fax: +385 1 612 98 32
E-mail: ignac.lovrek@fer.hr

The paper deals with verification of signalling protocols for telecommunication services. The model of signalling protocols synthesis based on elementary communicating processes and information flows they exchange is proposed. Elementary communicating processes represent basic service building blocks and exchange information by using process protocols. Service protocol is produced as a composition of process protocols for elementary processes involved. Verification problems related to elementary process protocols and service consistency are discussed. Some examples describing verification of signalling protocols for intelligent network are included.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 2

Web links: `http://www.hr/zzt/osoblje/Lovrek.html`

TESTING THEORY IN PRACTICE: A SIMPLE EXPERIMENT

Rinke Terpstra, Luis Ferreira Pires, Lex Heerink, and Jan Tretmans

Tele-Informatics and Open Systems Group
Department of Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede, The Netherlands
email: tretmans@cs.utwente.nl , pires@cs.utwente.nl , heerink@cs.utwente.nl
tel: +31 53 489 4287
fax: +31 53 489 3247

In this paper we discuss the experiences gained in conducting a simple testing experiment. The goal of this experiment is to apply the abstract, formal testing framework "Formal Methods in Conformance Testing" in a practical setting, and to indicate the critical aspects in its application to realistic testing situations. For that purpose a formal description of the system under test (SUT) is made from which tests are systematically derived. These tests are interpreted and executed by a tester against concrete implementations, thereby giving an indication about the correctness of these implementations.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 3

TESTING OF ISDN SERVICES BASED ON SDL SPECIFICATIONS

Marjeta Pucko

Jozef Stefan Institute
Digital communications and networks department
POB 3000, SI-1001 Ljubljana, Slovenia

Tel: +386 61 1773 724
Fax: +386 61 1262 102
E-mail: marjeta.pucko@ijs.si

Experiences in using formal methods in the practical example of automated derivation of test sequences for testing telecommunications services are described. The input of the first phase of the complete derivation process, where a logically correct SDL specification is generated, is an informal ETSI description, specifying the external behaviour of a given ISDN service. The informal-to-formal transformations in this phase are not completely automated. The output of its second phase is a set of automatically derived test sequences described in TTCN. Test sequences are generated using FSM-based methods.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 3

TEST SEQUENCE GENERATION BASED ON STOCHASTICS PROGRAMMING

P. Benczur (1), Geza Nemeth (2), Katalin Tarnay (2)

(1) ELTE TKK
(2) KFKI-MSZKI
Budapest
Hungary

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 3

A FUZZY MODEL FOR TEST RESULTS CERTIFICATION

Mihaly Bohus (1), Laszlo Koczy (2), Katalin Tarnay (3)

(1) Computer Department, JATE
~

(2) Department of Telecommunications and Telematics
Technical University of Budapest
~

(3) KFKI-MSZKI
Budapest
Hungary

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 3

FORMAL DESCRIPTION ON THE TEST DOCUMENT HIERARCHY

Ana Maria Ponce (1), Geza Nemeth (2), Janos Miskolczi (2), Katalin Tarnay (2)

(1) International Potato Center
Lima
Peru
~

(2) KFKI-MSZKI
Budapest
Hungary

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 3

TESTING X.400

Sarolta Dibuz(1), Abdulla K. Areik (2)

(1) KFKI Group , LNX Ltd.
Hun u. 2.
Budapest H-1135, Hungary
E-mail: dibuzs@lnx.hu
tel:+36-1-2660707
fax:+36-1-2660787
~

(2) Department of Telecommunications and Telematics
Technical University of Budapest
Muegyetem rkp.3.
Budapest H-1111, Hungary
tel:+36-1-463-1111

Conformance testing is an important step in protocol engineering. It is necessary to ensure the quality and interworking features of the protocol implementations. Conformance testing of protocols used in communication networks is always a complex and difficult task, and time-consuming. Even if the standardised test suit is availbale for the protocol. The paper presents an example of testing an application layer protocol, X.400, highlighting some properties of the protocol and the test suit for it.

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 3

VALIDATION OF COMMUNICATIONS PROTOCOLS

Gyula Csopaki

Technical University of Budapest
Department of Telecommunications and Telematics
H-1521, Budapest Pf. 91.
Hungary

Tel: +36-1-463 2589
fax: +36-1-463 3107
E-mail: csopaki@bme-tel.ttt.bme.hu

During the last ten years, validation technology has developed from being a research topic to a practical method of finding errors in complex distributed system and is now available as part of several, commercially available software development tools. The formal validation of system specifications is accepted by equipment manufacturers as a significant means of avoiding the costs of design error.

Validation is the collection of appropriate methods, procedures and tools used to evaluate that a specification:

- *satisfies the purpose expressed in the record of requirements on which the standard is based;*
- *can be fully implemented;*
- *when implemented, is able to offer all the functionality and performance expressed in the record of requirements of the standard it is based on;*
- *conforms to the established criteria for standards.*

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 3

MHS MESSAGE WITH EDIM

Gabor Borsodi (1), Sarolta Dibuz (2), Katalin Tarnay (3)

(1) Department of Telecommunications and Telematics
Technical University of Budapest
~
(2) KFKI Group
~
(3) KFKI-MSZKI
Budapest
Hungary

This presentation has been given during the COST-247 International Workshop on Applied Formal Methods in System Design (Maribor, Slovenia, June 17–19, 1996).

COST-247 Working Group(s): 3

An operational characterisation of may- and must-test in ET-LOTOS

Luc Leonard

Universite de Liege
Systemes et Automatique
Institut Montefiore, bat. B28
B4000 Liege
Belgium
Tel: 32 43 66 49 92
Fax: 32 43 66 29 89
E-mail: leonard@montefiore.ulg.ac.be

ET-LOTOS is an extension of LOTOS allowing the modelling of time-sensitive systems (i.e. systems whose behaviour is influenced by the passing of time). It is designed to be a "user friendly" formalism permitting the description of time dependent mechanisms in a clean and elegant manner, without having to resort to "tricks" and complex constructs. The counter-part of this rich expressive capability is that "undesirable" behaviours can be specified as well. For example, some processes cannot progress in time. Others enter in "zeno" divergences: they progress towards a certain time without ever reaching it. Other unrealistic behaviours are in fact desired features of the language: e.g. the possibility to perform consecutive actions at a same time instant is a useful abstraction.

Test has already been studied for other timed formalisms. However it was always under restrictive hypothesis withdrawing precisely the "unrealistic" behaviours evoked above. Then, this is where our contribution takes place. We present fully abstract characterisations of may- and must-test in ET-LOTOS, taking into account all the possible behaviours, and we show how to derive them from the semantics of the processes, i.e. from their LTS.

This presentation has been given during the COST-247 9th Management Committee

Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s):

Web links: `http://www-run.montefiore.ulg.ac.be`

Complexity of Estelle specifications

Jean-Luc Raffy

Institut National des Telecommunications (INT)
Les Epinettes
9, rue Charles Fourier
91011 EVRY cedex
FRANCE

We will present a set of metrics designed to evaluate the complexity of Estelle specifications. We first identify three different sources of complexity with respect to three different views of an Estelle specification. Then we propose metrics which permit to assess the complexity at each level. Finally, we will present the results of the metrics for several specifications.

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s):

State Space Reduction of SDL with Partial-Order Methods

Alper Sen

TUBITAK Software R&D Center
Department of Electrical and Electronics Engineering,
Middle East Technical University,
Ankara, Turkey
E-mail: sen@srdc.metu.edu.tr
Tel:+90-312-2101298
Fax:+90-312-2101411

State space generated during verification of protocols is usually so large that most of the time because of memory limitations verification is not completed. This problem is also known as the state-explosion problem. I worked on partial-order methods which make use of the modelling of concurrency by interleaving. We developed methods specifically for SDL systems one of which is read-first strategy saying that whenever an SDL process is at an input state then generate the exploration tree by expanding only this transition. This in fact leads to a great amount of reduction. Results for the effect of the methods have been illustrated by a new verification tool POVSDL. It has also been observed that POVSDL performs always better than commercial verifiers.

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s): 2

Web links: `http://www.srdc.metu.edu.tr/~sen/`

A verification of a distributed summing protocol

Jan Friso Groote

Centrum voor Wiskunde en Informatica
Specification and Analysis of Embedded Systems
P.O. Box 94079
1090 GB Amsterdam
The Netherlands

Tel. +31-20-5924232
Fax. +31-20-5924199
E-mail: jfg@cwi.nl

We provide a verification of the distributed summing protocol using the cones and foci method. The protocol works in the context of a arbitrary connected network, where each node contains a number. The goal of the protocol is to let the root report the sum of the numbers of all elements. The protocol is interesting because it works in a highly nondeterministic way; althought the outcome is determined, it is unkown in what way it is obtained. It shows that the cones and foci method is capable of these kind of verifications. It should be noted that the proof that has been provided is based on process algebraic axioms and rules and as such can straightforwardly been computer checked (note added september 1998: the proof has been completely computer checked using PVS leading to one additional invariant and minor changes in another invariant).

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s):

Specification and Verification of the PowerScale(TM) Bus Arbitration Protocol: An Industrial Experiment with LOTOS

Gh. Chehaibar, H. Garavel, L. Mounier, N. Tawbi, F. Zulian

INRIA Rhone-Alpes / Dyade / Verimag
655, avenue de l'Europe
38330 MONTBONNOT ST MARTIN
FRANCE
tel: +(33) 4 76 61 52 24
fax: +(33) 4 76 61 52 52
E-mail: hubert.garavel@inria.fr

This talk presents the results of an industrial case-study concerning the use of formal methods for the validation of hardware design. The case-study focuses on PowerScale, a multiprocessor architecture based on PowerPC(*) micro-processors and used in Bull's Escala series of servers and workstations. The specification language LOTOS (ISO International Standard 8807) was used to describe formally the main components of this architecture (processors, memory controller and bus arbiter).

Four correctness properties were identified, which express the essential requirements for a proper functioning of the arbitration algorithm, and formalized in terms of bisimulation relations (modulo abstractions) between finite labelled transition systems. Using the compositional and on-the-fly model-checking techniques implemented in the CADP (CAESAR/ALDEBARAN) toolbox, the correctness of the arbitration algorithm was established automatically in a few minutes.

(*) PowerScale and Escala are registered trademarks of Bull. PowerPC is a registered trademark of the International Business Machines Corporation.

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s):

Web links: `http://www.inrialpes.fr/vasy`

About compositional verification of TLA protocol specifications using projections

Tatjana Kapus, Zmago Brezocnik

Faculty of Electrical Engineering and Computer Science
University of Maribor
Smetanova ul. 17, SI-2000 Maribor, Slovenia
Email: kapus@uni-mb.si , brezocnik@uni-mb.si
Tel: +386 62 221-112
Fax: +386 62 225-013

A common approach to reduce the complexity of the verification of a concurrent system or algorithm is to decompose it into smaller parts and to verify each part separately. Although communication protocol entities typically perform several distinct functions, it has long been observed that it is often difficult to decompose them into smaller separate modules for handling each function because they share variables and/or messages. The method of projections has been proposed as an alternative. We show how projections can be performed in combination with compositional proof rules for verifying (interleaving) parallel compositions of components specified in the style of TLA. In fact, projection is implication.

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s):

Using CSP for authentication protocol analysis: the Needham-Schroeder Public Key Protocol

Steve Schneider

Royal Holloway, University of London
Egham, Surrey, TW20 0EX, UK
E-Mail: steve@dcs.rhbnc.ac.uk
tel: +44 1784 443431
fax: +44 1784 439786

This talk presents a general approach for analysis and verification of authentication properties in CSP. It is illustrated by an examination of the Needham-Schroeder Public-Key protocol. The paper aims to develop a specific theory appropriate to the analysis of authentication protocols, built on top of the general CSP semantic framework. This approach aims to combine the ability to express such protocols in a natural and precise way with the ability to reason formally about the properties they exhibit.

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s):

Web links: `http://www.dcs.rhbnc.ac.uk/research/formal/steve.html`

Extended Markovian Bisimulation Equivalence

Marco Bernardo

Universita' di Bologna
Dipartimento di Scienze dell'Informazione
Mura Anteo Zamboni 7
40127 Bologna
Italy
E-mail: bernardo@cs.unibo.it
Tel: +39 51 354516
Fax: +39 51 354510

EMPA enhances the expressiveness of classical process algebras by integrating functional and performance descriptions of concurrent systems. This is achieved by offering, besides passive actions (useful for pure nondeterminism), actions whose duration is exponentially distributed as well as immediate actions (useful for performance abstraction), parametrized by priority levels (hence prioritized choices) and weights (hence probabilistic choices). In order to analyze an EMPA term, from its integrated semantic model (a transition system labeled on both action types and action durations) we derive a functional semantic model (a transition system labeled on action types only) and a performance semantic model (a Markov chain). We show that an integrated analysis, i.e. a notion of equivalence on the integrated semantic model, is not only convenient but also necessary to achieve compositionality.

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s): 1-4

Web links: `http://www.cs.unibo.it/~bernardo`

Animation of real-time ET-LOTOS specifications

Christian Hernalsteen and Antony De Jacquier

Universite Libre de Bruxelles
Departement d'Informatique, CP212
Bl. du Triomphe
Brussels, Belgium
e-mail: chernals@ulb.ac.be
tel: +32 2 650 50 42
fax: +32 2 650 56 09

Formal description techniques based on process algebras allow the precise and succinct description of complex reactive systems. Such specifications are concise and unambiguous but are sometimes difficult to understand. Tools like animators are then useful for the correct understanding and the design of a specification. An animator allows the step by step execution of the system description in order to insure that what is formally described is really what was desired. This allows the detection of design errors at early stages of the system development. We have developed a tool called SELTA (for Simulator of ET-LOTOS based on Timed Automaton) which allows the animation of ET-LOTOS specifications. ET-LOTOS is a timed extension of the formal description technique LOTOS. This language allows the specification of real-time systems where timing evolution can modify the behavior of the system. This timed extension is currently considered by the ISO work-group dedicated to the revision of the LOTOS standard (E-LOTOS).

The tool supports all the ET-LOTOS operators. The data part has not been implemented, only the rational data type can be used. SELTA allows the animation of the specification by offering to the user the possible evolutions of the system. At each step, the user must choose between the firing of an enabled action and the timed evolution of the system. The animator supplies information to the user at each step:

- *The elapsed time since the beginning of the animation.*

- *The maximal possible progress in time of the currently animated behavior. This information shows that an action is urgent (Internal actions are urgent in ET-LOTOS).*
- *The next important moment in the system's life. The tool can determine the amount of time by which the system must age to change the set of enabled actions.*

The possibility to determine the next moment where the system changes its state gives the tool its power. This information helps the user to manage his specification animation by showing the important moments of the system evolution.

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s):

Refinement of Lotos specifications

Timo Karvi

Department of Computer Science
PO Box 26 (Teollisuuskatu 23)
FIN-00014 UNIVERSITY OF HELSINKI
FINLAND
E-mail: Timo.Karvi@cs.Helsinki.FI

It can be claimed that current Lotos environments don't support sufficiently the design of a large specification. Given the requirements and service specification of a protocol, a good Lotos environment should help to develop the final specification gradually step by step. At each step, it should also be possible to verify that the correct final specification is reachable, at least in principle. In this talk we pay attention to the CCS-related works of Celikkan, Cleaveland and Steffen. We examine their notion of partially defined specifications and show its usefulness also with respect to Lotos. However, there are some problems in applying the concept to specifications in full Lotos.

This presentation has been given during the COST-247 9th Management Committee Meeting (Antalya, Turkey, November 4–5, 1996).

COST-247 Working Group(s):

Experiences with practical protocol testing

Krzysztof M. Brzezinski, Marek Sredniawa

Institute of Telecommunications
Warsaw University of Technology
Nowowiejska Str. 15/19
00-665 Warsaw
Poland
Tel: +48 22 259 820
Fax: +48 22 254 950
E-mail: kb@tele.pw.edu.pl

The paper reports on the initial experience with practical aspects of conformance testing, gained at the Laboratory of Testing and Verification, Inst. of Telecommunications, with respect to ISDN subscriber signalling protocols (DSS1). Test standardization issues are surveyed. A particular niche application of conformance testing methodology is identified to deal with the case in which standardized test suites are absent and full formality of the testing process is not expected, yet some preliminary results are required quickly. As a tool support for such niche applications, we have put forward a concept of a simple and flexible protocol tester PMM, equipped with internal test generation functions. The design of the experimental PMM tool is briefly discussed. Experiences with testing of four different implementations of the DSS1 network side are reported, for both manually and semi-automatically generated test suites.

This presentation has been given during the COST-247 3rd Management Committee Meeting (Evry, France, September 19–20, 1994).

COST-247 Working Group(s): 3

Software Development in Telecommunications - Problems and Challenges

Kristian Toivo (1), Antun Caric (2)

(1) Oy LM Ericsson Ab
Telecom R&D
FIN-02420 Jorvas
Finland
Tel: +358 9 299 2752
E-mail: kristian.toivo@lmf.ericsson.se

(2) Ericsson Nikola Tesla
Design Center
Krapinska 45
HR-10000 Zagreb
Croatia
Tel: + 385 1 326 513
Fax: + 385 1 328 540
E-mail: etk.etkcar@memo.ericsson.se

New national and/or global operators with severe mutual competition apper as a direct conseguence of telecommunication market liberalization and deregulation. This has resulted in new reguirements on telecommunication networks and with increased reqirements on quality, cost and lead time for development of telecommunication systems. R&D institutions and/or units are nowadays faced with continuos but accelerated changes as prerequisites for their own survival or survival of their companies or corporation. Super fast development processes, significant improvement in competence and productivity, CMM based process improvement, new development models, extremely low software fault density supporting "zero down time" etc. are just examples of needed changes. Response on above mentioned problems and challenges are presented in the paper through cooperation between Ericsson Finland and Ericsson Nikola Tesla, Croatia, as case study.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s): 2

A Tool Framework for Verifying Concurrent Systems

Rance Cleaveland, Steve Sims

Department of Computer Science
North Carolina State University
Raleigh, NC 27695-8206 USA

Tel: +1 919 515 7862
Fax: +1 919 515 7896
E-mail: rance@csc.ncsu.edu

Despite the enormous strides made in automatic verification technology over the past decade and a half, tools such as model checkers remain relatively underused in the development of software. One reason for this is that the bewildering array of specification and verification formalisms complicates the development and adoption by users of relevant tool support. This paper proposes a remedy to this state of affairs in the case of finite-state concurrent systems by describing an approach to developing customizable yet efficient verification tools.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

Web links: `http://www4.ncsu.edu/~rance/WWW/`

Verification using Leap Automata

H. Yenigun(1), K. Inan (2)

(1) Bell Laboratories
Lucent Technologies
700 Mountain Avenue, Murray Hill
NJ 07974, USA
Tel: +1-908-582 6165
Fax: +1-908-582 5857
E-Mail: husnu@research.bell-labs.com
~
(2) Electrical & Electronics Engineering Department
Middle East Technical University
Balgat-Ankara
Turkey
Tel: +90-312-210 1298
Tel: +90-312-210 1411
E-mail: inan@srdc.metu.edu.tr

Transition leaping mechanism is presented in the literature as an additional and powerful complexity reducing mechanism used together with partial order methods for finite state verification. In this paper we improve on the original leaping approach by setting it in a more general context thereby enhancing the potential for greater complexity reduction. In particular by allowing ample sets that are not necessarily disjoint we present leaping results both for safety and liveness verification where the latter is presented only under a fairness assumption.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

A Practical Approach to Testing Finite State Systems

D. Larrabeiti, J. Quemada, S. Pavn

Dept. of Telematic Engineering
Technical University of Madrid
Ciudad Universitaria
Madrid 28040
Spain

Tel: +34 1 5495700
Fax: +34 1 3367333
E-mail: dlarra@dit.upm.es , jquemada@dit.upm.es , spavon@dit.upm.es

This paper presents a variation of the testing equivalence that provides an intuitive practical framework to test LOTOS behaviours whose infinite executions can be expressed in terms of successions of cycles. The proposal targets:

- *discriminating behaviours according to the relation between divergencies and successful terminations, introducing a fair interpretation of divergencies, and*
- *enabling a better knowledge of liveness properties of the system by means of cyclic tests.*

This features are being incorporated in the LOLA tool (LOTOS LAboratory)

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s): 1

Web links: `http://www.dit.upm.es/~dlarra`

New Features, Applications and Perspectives for the CADP'97 Toolbox

Hubert Garavel, M. Jorgensen, R. Mateescu, Ch. Pecheur, M. Sighireanu, B. Vivien

INRIA Rhone-Alpes
655 avenue de l'Europe
F-38330 Montbonnot Saint Martin
France
Tel : +(33) 4 76 61 52 24
Fax : +(33) 4 76 61 52 52
E-mail: Hubert.Garavel@inria.fr

This article gives an overview of the most recent features implemented in CADP (CAESAR/ALDEBARAN Development Package), a toolbox dedicated to the design and ve rification of communication protocols and distributed systems. Besides the desc ription of the new features, this paper also lists the latest applications of CA DP to industrial case-studies and mentions the current research directions for i mproving CADP.

COST-247 Working Group(s):

Web links: `http://www.inrialpes.fr/vasy`

MSCtool: Message Sequence Chart Specification and Verification using PROMELA/SPIN

Ignac Lovrek, Damir Jelavic, Martin Pavelic, Enes Dautovic, Emina Filipovic, Kresimir Madunovic

University of Zagreb
Faculty of Electrical Enginering and Computing
Unska 3
HR-10000 Zagreb
Croatia

Tel: +385 1 612 98 02
Fax: +385 1 612 98 32
E-mail: ignac.lovrek@fer.hr

The paper deals with a specification toll based on Message Sequence Chart and Message Sequence Chart verification using PROMELA/SPIN tool set. Basic features of Message Sequence Chart language as well as graphical and textual representation are listed. Message Sequence Chart editor, translator from graphical to textual form and PROMELA code generator as basic components of the MSCtool are described. Simple specification and verification examples are included.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s): 2

Web links: `http://www.hr/zzt/osoblje/Lovrek.html`

Software Tools for Technology Transfer

Bernhard Steffen(1), Rance Cleaveland(2)

(1) Fakultet fuer Mathematik und Informatik
Universitaet Passau
D-94030 Passau
Innstrasse 33
Germany
Tel: +49 851 509-3091
Fax: +49 851 509-3092
E-mail: steffen@fmi.uni-passau.de
~

(2) Department of Computer Science
North Carolina State University
Raleigh, NC 27695-7534
USA
Tel: +1 919 515-7862
Fax: +1 919 515-7925
E-mail: rance@csc.ncsu.edu

The MetaFrame tool integration platform is designed for the interactive combination and coordination of heterogeneous tools: complex tool combinations can be (semi-) automatically or interactively constructed and tested by on-line 'meta-programming' in the interpreted, sequential tool coordination language HLL. The point of our design is the strict separation of a highly enhanced integration phase and a strongly supported coordination phase. This allows even non-experts to profitably coordinate the integrated tools to solve their own application-specific tasks. It is this profile which qualifies our coordination environment to serve as the Electronic Tool Integration (ETI) platform in the new international Springer Journal Software Tools for Technology Transfer (STTT).

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s): 2

Web links: `http://www.csc.ncsu.edu/faculty/RCleaveland/`

Description and Formal Specification of the Link Layer of P1394

Bas Luttik

Center for Mathematics and Computer Science (CWI)
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands.

Programming Research Group, University of Amsterdam,
Kruislaan 403, 1098 SJ Amsterdam, The Netherlands.

Tel: +31 20 592 4247
Fax: +31 20 592 4199
E-mail: luttik@cwi.nl

We give a formal specification in μCRL of the Link Layer as described in the IEEE Standard P1394 that may serve as a starting point for further verification.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

Web links: `http://www.cwi.nl/~luttik/`

Validation of the Link Layer Protocol of the IEEE-1394 Serial Bus (FireWire): an Experiment with E-LOTOS

M. Sighireanu, R. Mateescu

INRIA Rhone-Alpes
655 avenue de l'Europe
F-38330 Montbonnot Saint Martin
France

Tel: +(33) 4 76 61 52 89
Fax: +(33) 4 76 61 52 52
E-mail: Mihaela.Sighireanu@inria.fr , Radu.Mateescu@inria.fr

This paper deals with the description in E-LOTOS of the asynchronous LINK layer protocol of the IEEE-1394 Standard and its verification using model-checking. The E-LOTOS descriptions are based on both the standard and the mu-CRL description written by Luttik. The verifications are performed using the CADP (CAESAR/ALDEBARAN) toolbox. We translate the E-LOTOS descriptions in LOTOS using the TRAIAN tool, and then we generate the underlying LTS models corresponding to various scenarios using the CAESAR compiler. We formally express in the ACTL temporal logic the five correctness properties of the LINK layer protocol stated in natural language by Luttik and we verify them on the LTS models using the XTL model-checker. We detect and correct a potential deadlock caused by the ambiguous semantics of the state machines given in the standard, which can be misleading for implementors of the IEEE-1394 protocol.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

Web links: `http://www.inrialpes.fr/vasy`

Towards Mechanical Verification of Parts of the IEEE P1394 Serial Bus

Lars Kuehne (1), Jozef Hooman (2), Willem-Paul de Roever (1)

(1) Christian-Albrechts-Universitaet zu Kiel
Institut fuer Informatik
Preusserstr. 1-9
D-24105 Kiel
Germany
Tel: +49 431 5604-74
Fax: +49 431 566143
E-mail: lku@informatik.uni-kiel.de , wpr@informatik.uni-kiel.de
~

(2) Technical Applications Group
Computing Science Department
Eindhoven University of Technology
P.O. Box 513, NL-5600 MB Eindhoven
The Netherlands
Tel: +31 - 40 - 2474283
Fax: +31 - 40 - 2468508
E-mail: wsinjh@win.tue.nl

The IEEE P1394 Serial Bus standard provides high performance connections for data transfer between hardware components and is especially well suited for connecting multimedia devices. To achieve its mechanical verification, a high level specification is developed for the asynchronous part of the P1394 Link layer, using the verification tool PVS. We derive a formal framework which closely resembles the state machine approach used in the standard document. In this framework, a new parallel combinator characterizes synchronous message passing between transitions for which a set of messages is exchanged atomically. The combinator is mechanically checked for being commutative and associative. As expected, unclarities, ambiguities and unforseen properties need to be resolved in the specifica-

tion of the Link layer. To date, important Link Layer properties have been handproved using linear time temporal logic; the next aim of the authors is the mechanization of these proofs in PVS.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

Web links: `http://www.informatik.uni-kiel.de/~wpr/`

Probabilistic Extensions of TE-LOTOS

Zbigniew Huzar(1), Jan Magott(2)

Computer Science Department
Faculty of Informatics and Management,
Technical University of Wroceaw, Poland
Tel: (48) (71) 3203431
Fax: (48) (71) 211018

(2) Institute of Engineering Cybernetics
Faculty of Electronics,
Technical University of Wroceaw, Poland

E-mail: z.huzar@ci.pwr.wroc.pl , magott@ict.pwr.wroc.pl

TE-LOTOS is a candidate for a timed extension of formal description language LOTOS. In the present paper, we extend TE-LOTOS with a possibility of probabilistic generation of the timing restrictions of the actions, and probabilistic generation of the delay time. The action denotation is extended with probability distributions for action timing constraints. Additionally, probabilities are used to solve non-determinism in choice behaviour expressions in stochastic or deterministic way.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

Functionality Bipartition in Basic E-LOTOS

Monika Kapus-Kolar

Jozef Stefan Institute
Digital communications and networks department
POB 3000, SI-1001 Ljubljana, Slovenia

Tel: +(386) 61 1773 531
Fax: +(386) 61 1262 102
E-mail: monika.kapus-kolar@ijs.si

A functionality-bipartition transformation for basic E-LOTOS specifications is proposed which, given a specification of the required external behaviour (the expected service) of a system and a partitioning of the specified service actions among the two system components, derives behaviour of individual system components implementing the service.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s): 1

Validation of Hardware Implementations using Formal Description Techniques

G. Huecas (1), T. Robles (1), L.M. Gonzalez(2), J. Serrano (3)

(1) DIT-UPM
Technical University of Madrid
Ciudad Universitaria s/n
28040 Madrid SPAIN
Tel : +34 1 549 57 00 x 442
Fax : +34 1 336 73 33
E-mail: gabriel@dit.upm.es
~

(2) GMV S.A.
c/Isaac Newton, 11, 28760 Madrid SPAIN
E-mail: lmgonzalez@gmv.es
~

(3) CRISA S.A.
c/Torres Quevedo, 9, 28760 Madrid SPAIN
E-mail: serrano@crisa.es

In December 1996, a project called LVARTS was finished and delivered to the ESA. The goal was to validate a real system, namely ATAC, an ADA co-processor chip, running on a real board. The system was big enough to develop specific methodologies and tools, which are described in this paper. LOTOS was chosen to formally specify ATAC. The formal specification was used to produce test cases that were executed against the chip, after a completion process to obtain executable test cases.

COST-247 Working Group(s):

Requirements for Service Creation Environments

Nikolaos Kosmas, Kenneth J. Turner

Department of Computing Science
University of Stirling
Stirling FK8 4LA
Scotland

Tel: +44 1786 467420
Fax: +44 1786 464551
E-mail: nko@cs.stir.ac.uk , kjt@cs.stir.ac.uk

Service Creation Environments are the new frontiers in telecommunications. Efficient and reliable service creation is vital towards the evolution of the telecommunication domain as we move into Intelligent Networks. This paper discusses the concept of service creation environments and how it is related to the process of service creation. Additionally, a list of abstract requirements for service creation environments is outlined.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

Web links: `http://www.cs.stir.ac.uk/~nko`

An Annotational Extension of SDL 92 to Support a Formal Implementation Specification

Peter Langenümlrfer

Brandenburg University of Technology at Cottbus
Department of Computer Science
Chair of Computer Networks and Communication Systems
Postbox 10 13 44
D-03013 Cottbus
Germany
Email: pl@informatik.tu-cottbus.de
Phone/Fax.: +49 3 55 69 22 36

Although the software lifecycle is shortening and the importance of software development tools is increasing, implementation-oriented aspects are still ignored in formal description techniques (FDTs). Thereby the contribution of FDTs to efficient software development is shortened since mostly the implementation process is done by hand to result in a better performance. To remedy this problem we propose implementation oriented SDL (iSDL). iSDL represents an extention of SDL' 92 to include implementation aspects into the language. The extentions allow the co-specification of functional and implementational aspects.

Thereby a formal implementation specification is constructed. This shortens the time needed for the implementation and leads to a more efficient maintenance of the implementation. This joint specification of functional and implementation aspects eases the task of software engineers. It saves effort otherwise needed to implement the specification by hand and the maintenance of the implementation is easier than without iSDL.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

Web links: `http://www-rnks.informatik.tu-cottbus.de/ pl`

Understanding and Modelling the USB Hub

Dennis Dams(1), Rob Gerth(1), Loe Feijs(2), Gertjan Kamsteeg(3)

(1) Dept. of Math. & Comp. Science
Eindhoven Univ. of Technology
PO Box 513
5600 MB Eindhoven, The Netherlands
Tel: +31 40 247 5159/4389/4124
Fax: +31 40 246 3992
E-mail: wsindd@win.tue.nl , robg@win.tue.nl

(2) Philips Research Labs.
Prof. Holstlaan 4
5656 AA Eindhoven, The Netherlands
Tel: +31 40 274 2953
E-mail: feijs@natlab.research.philips.com

(3) Dept. of Comp. Science
Leiden Univ.
PO Box 9512
2300 RA Leiden, The Netherlands
E-mail: 106406.1504@compuserve.com

This paper describes our ongoing experiences during the a-posteriori formalisation of the USB hub protocol in Promela, and subsequent simulation and verification experiments. Such an activity forces one to consider all chosen aspects with equal (and great) precision. The paper focusses on the technical aspects of the model, the choices we had to make, and the problems we encountered. Many unclarities, inconsistencies and errors in the original text of the specification were uncovered.

This presentation has been given during the COST-247 2nd International Workshop on Applied Formal Methods in System Design (Zagreb, Croatia, June 18–19, 1997).

COST-247 Working Group(s):

Web links: `http://www.win.tue.nl/cs/fm/Loe.Feijs`

Specification and Verification of the CO4 Distributed Knowledge System using LOTOS

Charles Pecheur (presentation given by Hubert Garavel)

INRIA Rhone-Alpes
655 avenue de l'Europe
F-38330 Montbonnot Saint Martin
France
Tel: +33 4 76 61 52 98
Fax: +33 4 76 61 52 52
E-mail: Charles.Pecheur@inria.fr

This talk presents the specification and verification of a consensual decision protocol used in Co4, a computer environment dedicated to the building of a distributed knowledge base. This protocol has been specified in the ISO formal description technique LOTOS. The CADP tools from the EUCALYPTUS LOTOS toolset have been used to verify different safety and liveness properties. The verification work has confirmed an announced violation of knowledge consistency and has put forth a case of inconsistent hierarchy, four cases of unexpected message reception and some further local corrections in the definition of the protocol.

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Hardware-Software Co-Design for Protocols

Gyula Csopaki

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Relating Architecture and Specification

Ken Turner

Computing Science and Mathematics
University of Stirling
Stirling FK9 4LA
United Kingdom
Email: kjt@cs.stir.ac.uk
Tel: +44-1786-467-420
Fax: +44-1786-464-551

The problems of multiple specification languages for multiple architectures are discussed. It is concluded that an architectural semantics is of practical value in ensuring consistent and effective development of specifications. The approach is discussed in general and by examples, concentrating mainly on an architectural semantics for Open Systems Interconnection in relation to ESTELLE, LOTOS and SDL. It is shown how an architectural semantics can be realised using a library of specification templates, allowing the specifier to work at a higher, more architectural level. Some LOTOS templates are discussed, mainly for Open Systems Interconnection.

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Web links: `http://www.cs.stir.ac.uk/~kjt/research/`

Timed μCRL

Jan-Friso Groote

Centrum voor Wiskunde en Informatica
Specification and Analysis of Embedded Systems
P.O. Box 94079
1090 GB Amsterdam
The Netherlands
Email: jfg@cwi.nl
Tel. +31-20-5924232
Fax. +31-20-5924199

We explain how we extended mCRL with time in such a way that 'classic' mCRL specifications are valid timed mCRL specifications that only do not make an explicit reference to time. In essence the extension consists of a single at operator, denoted by @. For a process expression p and a time t, p@t means that the first action that p executes must be executed at time t. Using the sum operators and the conditionals, complex time constrains can be expressed. ¡P¿ Furthermore, a distinction has been introduced in the datatypes. In 'classic' mCRL it was only possible to specify that datatypes consisted of a set of constructors. In timed mCRL it is also possible to state that there are ordinary functions which cannot create new elements in the datatype.

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Web links: `http://www.cwi.nl/static/publications/reports/SEN-1997.html`

Test Case Selection

Katy Tarnay

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Testing Interoperability

Mazen Malek

KFKI Research Institute for Measurement
and Computing Techniques KFKI-MSZKI
Protocol Laboratory
H-1525 Budapest 114
P.O.Box 49 Hungary
E-mail: mazen@sun60.mszki.kfki.hu
Tel: (+36 1) 395-9220 / 26-84
Fax: (+36 1) 395-9027

The invention of protocols was to foster communication between computer systems, in such a way that users are no longer limited to have access to single type network, although support many features. Multi-vendor computer environment is a fact and to cope with the information exchange difficulties a need is required to standardized communicating protocols. The concept of assuring interoperability is getting more importance as information technology evolves. In this paper we try to focus on interoperability definitions and applicable ways of measuring it.

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Web links: `http://www.kfki.hu`

Testing at LTiV - Research and Application Projects

Krzysztof Brzezinski

Institute of Telecommunications
Warsaw University of Technology
Nowowiejska Str. 15/19
00-665 Warsaw
Poland
E-mail: kb@tele.pw.edu.pl
Tel: +48-22-660-74-96
Fax: +48-22-660-75-64

An account is given of the activities undertaken at the Laboratory of Testing and Verification (LTiV), Warsaw Univ. of Technology, within the framework of COST 247 action WG3. To address a number of fundamental and practical questions, a modular approach to testing is submitted. Conceptual modularity is dealt with by defining a new, efficient taxonomy of testing-related concepts and techniques. The technical aspect of modularity is addressed by decomposing MOT functions into a number of generic modules and composing these (separately implemented) modules to obtain a range of both traditional and novel test instruments. As an example of the application of proposed methodology, the PMM family of test modules is briefly described. The KODEKO signalling monitor is presented in detail.

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Firewire Tree Identify Protocol

Carron Shankland

Dept of Computing Science & Mathematics
University of Stirling
Stirling
FK9 4LA
Email: ces@cs.stir.ac.uk
Tel: +44 1786 467444
Fax: +44 1786 464551

In formal methods we are always searching for new and interesting examples to which we can apply our techniques. In this talk I will introduce a case study based on the Philips "firewire". (More specifically, the tree identify protocol of a high performance serial multimedia bus (IEEE standard 1394)). The description, given using muCRL, is made in varying levels of detail and I show, using the cones and foci technique of Groote and Springintveldt that these different descriptions are all equivalent under branching bisimulation. I'll also talk about the techniques used, and make some observations about properties of the protocol.

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Web links: `http://www.cs.stir.ac.uk/~ces`

Verification of VDM-Style Specifications with PVS

Savi Maharaj

Department of Computing and Mathematics
Stirling University
Stirling FK9 4LA
Scotland
E-mail: savi@cs.stir.ac.uk
Tel: +44 1786 467431
Fax: +44 1786 464551

In summer 1996, while visiting the Rutherford Appleton Laboratory in England, I hand-translated some medium sized VDM specifications into the PVS language and used the PVS prover to verify some properties of these specifications. The VDM specifications relate to the MSMIE[1] (Multiprocessor Shared-Memory Information Exchance) protocal which was designed for use in nuclear safety systems at Westinghouse, and specified in VDM by Juan Bicarregui at RAL[2].

¡P¿ This exercise showed that it is fairly straightforward to translate a large fragment of VDM into PVS. The methods used are essentially those described by Agerholm[3]. The translation may be done in such a way that some VDM proof obligations are generated automatically as TCCs in PVS. However the translation is only superficial — differences between the two logics mean that the semantics of VDM is not preserved. The translation may be extended to deal with refinement between specifications, at least in a superficial way, but the differences between the two logics mean that the VDM notion of refinement is not correctly captured.

¡P¿ Conclusions about the PVS system: it is relatively easy to learn to use, and quite fast at doing proofs, and it has a very useful and expressive specification language. However there are concerns about the lack of independently checkable proof objects, the difficulty of understanding the behaviour of the powerful tactics provided by the system, and the presence of bugs in the current implementation.

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1

Web links: `http://www.cs.stir.ac.uk/~sma/`

Use of Formal Methods in The BOS Project

Jan Tretmans

Tele-Informatics and Open Systems Group
Department of Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede, The Netherlands
Email: tretmans@cs.utwente.nl
Tel: +31 53 489 4287
Fax: +31 53 489 3247

A storm surge barrier is being built near Rotterdam: a movable dam in the Nieuwe Waterweg, the canal connecting Rotterdam with the sea, to protect Rotterdam from being flooded. BOS (in Dutch: Beslis- en Ondersteunend Systeem, i.e., decision and support system) is the computer system that should fully autonomously decide about closing of the barrier and execute the procedure for closing the barrier. CMG Den Haag B.V., responsible for building the software of BOS, decided to use formal methods as one of the means to meet the high safety and reliabilty requirements on BOS. Advised by the University of Twente, CMG selected SPIN/Promela and Z to be used for technical design and validation of the crucial parts of the software. This presentation will report about the experiences with the use of formal methods in the BOS project.

This presentation has been given during the COST-247 Project Management Committee Meeting (Stirling, United Kingdom, October 13–14, 1997)

COST-247 Working Group(s): 1