Nabil Abdennadher
Fabrice Kordon (Eds.)

LNCS 4498

Reliable Software Technologies – Ada-Europe 2007

12th Ada-Europe International Conference on Reliable Software Technologies Geneva, Switzerland, June 2007, Proceedings

Springer

Nabil Abdennadher Fabrice Kordon (Eds.)

Reliable Software Technologies – Ada-Europe 2007

12th Ada-Europe International Conference on Reliable Software Technologies
Geneva, Switzerland, June 25-29, 2007
Proceedings

Springer

Volume Editors

Nabil Abdennadher
University of Applied Sciences Western Switzerland, HES.SO
École d'ingénieurs de Genève
Rue de la Prairie 4, 1202 Geneva, Switzerland
E-mail: Nabil.Abdennadher@hesge.ch

Fabrice Kordon
Université Pierre et Marie Curie
Laboratoire d'Informatique de Paris 6
104 Avenue du Président Kennedy, 75016 Paris, France
E-mail: Fabrice.Kordon@lip6.fr

Library of Congress Control Number: 2007929319

CR Subject Classification (1998): D.2, D.1.2-5, D.3, C.2.4, C.3, K.6

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-73229-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-73229-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12080861 06/3180 5 4 3 2 1 0

Preface

Reliable Software Technologies is an annual series of international conferences devoted to the promotion and advancement of all aspects of reliable software technologies. The objective of this series of conferences, initiated and sponsored by Ada-Europe, the European federation of national Ada societies, is to provide a forum to promote the development of reliable softwares both as an industrial technique and an academic discipline.

Previous editions of the Reliable Software Technologies conference were held in: Porto (Portugal) in 2006, York (UK) in 2005, Palma de Mallorca (Spain) in 2004, Toulouse (France) in 2003, Vienna (Austria) in 2002, Leuven (Belgium) in 2001, Potsdam (Germany) in 2000, Santander (Spain) in 1999, Uppsala (Sweden) in 1998, London (UK) in 1997 and Montreux (Switzerland) in 1996.

The 12th International Conference on Reliable Software Technologies took place in Geneva, Switzerland, June 25-29, 2007, under the continued sponsoring of Ada-Europe, in cooperation with ACM SIGAda. It was organized by members of the University of Applied Sciences, Western Switzerland (Engineering School of Geneva), in collaboration with colleagues from various places in Europe. The 13th conference, in 2008, will take place in Venice, Italy.

Continuing the success achieved in previous years, the conference included a three-day technical program, where the papers contained in these proceedings were presented. The technical program was bracketed by two tutorial days where attendants had the opportunity to catch up on a variety of topics related to the fields covered by the conference, at both introductory and advanced levels. The technical program also included an industrial track, with contributions illustrating challenges faced and solutions devised by industry from both sides of the Atlantic, as well as from the rest of the world (we note several contributions from South-East Asia). Furthermore, the conference was accompanied by an exhibition where vendors presented their products for supporting the development of reliable software.

The conference featured four distinguished speakers, who delivered state-of-the-art information on topics of great importance, both for the present and the future of software engineering:

- Challenges for Reliable Software Design in Automotive Electronic Control Units *by Klaus D. Mueller-Glaser (University of Karlsruhe, Germany)*
- Synchronous Techniques for Embedded Systems *by Gerard Berry (Esterel Technologies, France)*
- Perspectives on Next-Generation Software Engineering *by Ali Mili (New Jersey Institute of Technology, USA)*
- Observation Rooms for Program Execution Monitoring *by Liviu Iftode, (Rutgers University, USA)*

We would like to express our sincere gratitude to these distinguished speakers for sharing their insights with the conference participants.

A large number of regular papers were submitted, from as many as 15 different countries. The Program Committee worked hard to review them, and the selection process proved to be difficult, since many papers had received excellent reviews. The Program Committee eventually selected 18 papers for the conference and these proceedings.

The industrial track of the conference also received valuable contributions from industry, and the Industrial Committee selected nine of them for presentation in Geneva. The final result was a truly international program with contributions from Australia, Austria, China, France, Germany, Italy, Republic of Korea, Spain, Tunisia, and the UK, covering a broad range of topics: real-time systems, static analysis, verification, applications, reliability, industrial experience, compilers and distributed systems.

The conference also included an interesting selection of tutorials, featuring international experts who presented introductory and advanced material in the domain of the conference:

- An Overview of Model-Driven Engineering, *William Bail*
- CbyC: A UML2 Profile Enforcing the Ravsenscar Computational Model, *Tullio Vardanega*
- Verification and Validation for Reliable Software Systems, *William Bail*
- Object-Oriented Programming in Ada 2005, *Matthew Heaney*
- Security by Construction, *Rod Chapman*
- Synchronous Design of Embedded Systems: the Esterel/Scade Approach, *Gerard Berry*
- Building Interoperable Applications with PolyORB, *Thomas Quinot and Jérôme Hugues*
- Situational Method Engineering: Towards a Specific Method for Each System Development Project, *Jolita Ralyté*

We wish to extend our gratitude to these experts for the work they put into preparing and presenting this material during the conference.

The 12th Reliable Software Technologies (Ada-Europe 2007) conference was made possible through the generous support and diligent work of many individuals and organizations. A number of institutional and industrial sponsors also made important contributions and participated in the industrial exhibition. Their names and logos appear on the Ada-Europe 2007 Web site.We gratefully acknowledge their support. A subcommittee comprising Nabil Abdennadher, Dirk Craeynest, Fabrice Kordon, Dominik Madon, Ahlan Marriott, Tullio Vardanega and Luigi Zaffalon met in Geneva to elaborate the final program selection. Various Program Committee members were assigned to shepherd some of the papers. We are grateful to all those who contributed to the technical program of the conference.

We would like to thank the members of the Organizing Committee for their valuable effort in taking care of all the details needed for a smooth run of the

conference. Dominik Madon did a superb job in organizing an attractive tutorial program. Luigi Zaffalon took on the difficult task of preparing the industrial track. We would also like to thank Dirk Craeynest and Ahlan Marriott, who worked very hard to make the conference prominently visible, and to all the members of the Ada-Europe board for helping with the intricate details of the organization. Special thanks go to Régis Boesch and Albena Basset, who took care of all details of the local organization.

Finally, we also thank the authors of the contributions submitted to the conference, and to all the participants who helped in achieving the goal of the conference: to provide a forum for researchers and practitioners for the exchange of information and ideas about reliable software technologies. We hope they all enjoyed the program as well as the social events of the 12th International Conference on Reliable Software Technologies.

June 2007

Nabil Abdennadher
Fabrice Kordon

Organization

Conference Chair

Nabil Abdennadher, University of Applied Sciences, Geneva, Switzerland

Program Co-chairs

Nabil Abdennadher, University of Applied Sciences, Geneva, Switzerland
Fabrice Kordon, Université Pierre & Marie Curie, Paris, France

Industrial Committee Chair

Luigi Zaffalon, University of Applied Sciences, Geneva, Switzerland

Tutorial Chair

Dominik Madon, University of Applied Sciences, Geneva, Switzerland

Exhibition Chair

Neville Rowden, Siemens Switzerland

Publicity Co-chairs

Ahlan Marriott, White-elephant, Switzerland
Dirk Craeynest, Aubay Belgium and K.U.Leuven, Belgium

Local Chair

Régis Boesch, University of Applied Sciences, Geneva, Switzerland

Ada-Europe Conference Liaison

Fabrice Kordon, Université Pierre et Marie Curie, Paris, France

Program Committee

Abdennadher Nabil, University of Applied Sciences, Geneva, Switzerland
Alonso Alejandro, Universidad Politécnica de Madrid, Spain
Asplund Lars, Mälardalens Högskola, Sweden
Barnes Janet, Praxis High Integrity Systems, UK

Blieberger Johann, Technische Universität Wien, Austria
Boasson Maartin, University of Amsterdam, The Netherlands
Burgstaller Bernd, University of Sydney, Australia
Craeynest Dirk, Aubay Belgium and K.U.Leuven, Belgium
Crespo Alfons, Universidad Politécnica de Valencia, Spain
Devillers Raymond, Université Libre de Bruxelles, Belgium
González Harbour Michael, Universidad de Cantabria, Spain
Gutiérrez José Javier, Universidad de Cantabria, Spain
Hadded Serge, Université Paris-Dauphine, France
Hately Andrew, Eurocontrol CRDS, Hungary
Hommel Günter, Technische Universität Berlin, Germany
Keller Hubert, Institut für Angewandte Informatik, Germany
Kermarrec Yvon, ENST Bretagne, France
Kienzle Jörg, McGill University, Canada
Kordon Fabrice, Université Pierre et Marie Curie, France
Llamosi Albert, Universitat de les Illes Balears, Spain
Lundqvist Kristina, MIT, USA
Mazzanti Franco, ISTI-CNR Pisa, Italy
McCormick John, University of Northern Iowa, USA
Michell Stephen, Maurya Software, Canada
Miranda Javier, Universidad Las Palmas de Gran Canaria, Spain
Moldt Daniel, University of Hamburg, Germany
Pautet Laurent, Telecom Paris, France
Petrucci Laure, LIPN, Université Paris 13, France
Pinho Luís Miguel, Polytechnic Institute of Porto, Portugal
Plödereder Erhard, Universität Stuttgart, Germany
de la Puente Juan A., Universidad Politécnica de Madrid, Spain
Real Jorge, Universidad Politécnica de Valencia, Spain
Romanovsky Alexander, University of Newcastle upon Tyne, UK
Rosen Jean-Pierre, Adalog, France
Ruiz José, AdaCore, France
Schonberg Edmond, New York University and AdaCore, USA
Seinturier Lionel, INRIA Lille, France
Shing Man-Tak, Naval Postgraduate School, USA
Tokar Joyce, Pyrrhus Software, USA
Vardanega Tullio, Università di Padova, Italy
Wellings Andy, University of York, UK
Winkler Jürgen, Friedrich-Schiller-Universität, Germany
Zaffalon Luigi, University of Applied Sciences, Geneva, Switzerland

Sponsoring Institutions

Ada-Europe
AdaCore
Aonix
Ellidiss Sowftare
Green Hills Software Inc.
Praxis

PostFinance
Sun Microsystems
Siemens
Telelogic

Fédération des Entreprises Romandes
Swiss Informatics Society
The Quality Software Foundation

Lecture Notes in Computer Science 4498

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Lecture Notes in Computer Science

For information about Vols. 1–4471

please contact your bookseller or Springer

Vol. 4600: H. Comon-Lundh, C. Kirchner, H. Kirchner (Eds.), Rewriting, Computation and Proof. XVI, 273 pages. 2007.

Vol. 4591: J. Davies, J. Gibbons (Eds.), Integrated Formal Methods. IX, 660 pages. 2007.

Vol. 4588: T. Harju, J. Karhumäki, A. Lepistö (Eds.), Developments in Language Theory. XI, 423 pages. 2007.

Vol. 4583: S.R. Della Rocca (Ed.), Typed Lambda Calculi and Applications. XI, 395 pages. 2007.

Vol. 4581: A. Petrenko, M. Veanes, J. Tretmans, W. Grieskamp (Eds.), Testing of Software and Communicating Systems. XII, 379 pages. 2007.

Vol. 4574: J. Derrick, J. Vain (Eds.), Formal Techniques for Networked and Distributed Systems – FORTE 2007. XI, 375 pages. 2007.

Vol. 4573: M. Kauers, M. Kerber, R. Miner, W. Windsteiger (Eds.), Towards Mechanized Mathematical Assistants. XIII, 407 pages. 2007. (Sublibrary LNAI).

Vol. 4572: F. Stajano, C. Meadows, S. Capkun, T. Moore (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. X, 247 pages. 2007.

Vol. 4569: A. Butz, B. Fisher, A. Krüger, P. Olivier, S. Owada (Eds.), Smart Graphics. IX, 237 pages. 2007.

Vol. 4549: J. Aspnes, C. Scheideler, A. Arora, S. Madden (Eds.), Distributed Computing in Sensor Systems. XIII, 417 pages. 2007.

Vol. 4548: N. Olivetti (Ed.), Automated Reasoning with Analytic Tableaux and Related Methods. X, 245 pages. 2007. (Sublibrary LNAI).

Vol. 4547: C. Carlet, B. Sunar (Eds.), Arithmetic of Finite Fields. XI, 355 pages. 2007.

Vol. 4546: J. Kleijn, A. Yakovlev (Eds.), Petri Nets and Other Models of Concurrency – ICATPN 2007. XI, 515 pages. 2007.

Vol. 4543: A.K. Bandara, M. Burgess (Eds.), Inter-Domain Management. XII, 237 pages. 2007.

Vol. 4542: P. Sawyer, B. Paech, P. Heymans (Eds.), Requirements Engineering: Foundation for Software Quality. IX, 384 pages. 2007.

Vol. 4541: T. Okadome, T. Yamazaki, M. Makhtari (Eds.), Pervasive Computing for Quality of Life Enhancement. IX, 248 pages. 2007.

Vol. 4539: N.H. Bshouty, C. Gentile (Eds.), Learning Theory. XII, 634 pages. 2007. (Sublibrary LNAI).

Vol. 4538: F. Escolano, M. Vento (Eds.), Graph-Based Representations in Pattern Recognition. XII, 416 pages. 2007.

Vol. 4537: K.C.-C. Chang, W. Wang, L. Chen, C.A. Ellis, C.-H. Hsu, A.C. Tsoi, H. Wang (Eds.), Advances in Web and Network Technologies, and Information Management. XXIII, 707 pages. 2007.

Vol. 4536: G. Concas, E. Damiani, M. Scotto, G. Succi (Eds.), Agile Processes in Software Engineering and Extreme Programming. XV, 276 pages. 2007.

Vol. 4534: I. Tomkos, F. Neri, J. Solé Pareta, X. Masip Bruin, S. Sánchez Lopez (Eds.), Optical Network Design and Modeling. XI, 460 pages. 2007.

Vol. 4531: J. Indulska, K. Raymond (Eds.), Distributed Applications and Interoperable Systems. XI, 337 pages. 2007.

Vol. 4530: D.H. Akehurst, R. Vogel, R.F. Paige (Eds.), Model Driven Architecture- Foundations and Applications. X, 219 pages. 2007.

Vol. 4529: P. Melin, O. Castillo, L.T. Aguilar, J. Kacprzyk, W. Pedrycz (Eds.), Foundations of Fuzzy Logic and Soft Computing. XIX, 830 pages. 2007. (Sublibrary LNAI).

Vol. 4528: J. Mira, J.R. Álvarez (Eds.), Nature Inspired Problem-Solving Methods in Knowledge Engineering, Part II. XXII, 650 pages. 2007.

Vol. 4527: J. Mira, J.R. Álvarez (Eds.), Bio-inspired Modeling of Cognitive Tasks, Part I. XXII, 630 pages. 2007.

Vol. 4526: M. Malek, M. Reitenspieß, A. van Moorsel (Eds.), Service Availability. X, 155 pages. 2007.

Vol. 4525: C. Demetrescu (Ed.), Experimental Algorithms. XIII, 448 pages. 2007.

Vol. 4524: M. Marchiori, J.Z. Pan, C.d.S. Marie (Eds.), Web Reasoning and Rule Systems. XI, 382 pages. 2007.

Vol. 4523: Y.-H. Lee, H.-N. Kim, J. Kim, Y. Park, L.T. Yang, S.W. Kim (Eds.), Embedded Software and Systems. XIX, 829 pages. 2007.

Vol. 4522: B.K. Ersbøll, K.S. Pedersen (Eds.), Image Analysis. XVIII, 989 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4519: E. Franconi, M. Kifer, W. May (Eds.), The Semantic Web: Research and Applications. XVIII, 830 pages. 2007.

Vol. 4517: F. Boavida, E. Monteiro, S. Mascolo, Y. Koucheryavy (Eds.), Wired/Wireless Internet Communications. XIV, 382 pages. 2007.

Vol. 4516: L. Mason, T. Drwiega, J. Yan (Eds.), Managing Traffic Performance in Converged Networks. XXIII, 1191 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4514: S.N. Artemov, A. Nerode (Eds.), Logical Foundations of Computer Science. XI, 513 pages. 2007.

Vol. 4513: M. Fischetti, D.P. Williamson (Eds.), Integer Programming and Combinatorial Optimization. IX, 500 pages. 2007.

Vol. 4511: C. Conati, K. McCoy, G. Paliouras (Eds.), User Modeling 2007. XVI, 487 pages. 2007. (Sublibrary LNAI).

Vol. 4510: P. Van Hentenryck, L. Wolsey (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 391 pages. 2007.

Vol. 4509: Z. Kobti, D. Wu (Eds.), Advances in Artificial Intelligence. XII, 552 pages. 2007. (Sublibrary LNAI).

Vol. 4508: M.-Y. Kao, X.-Y. Li (Eds.), Algorithmic Aspects in Information and Management. VIII, 428 pages. 2007.

Vol. 4507: F. Sandoval, A. Prieto, J. Cabestany, M. Graña (Eds.), Computational and Ambient Intelligence. XXVI, 1167 pages. 2007.

Vol. 4506: D. Zeng, I. Gotham, K. Komatsu, C. Lynch, M. Thurmond, D. Madigan, B. Lober, J. Kvach, H. Chen (Eds.), Intelligence and Security Informatics: Biosurveillance. XI, 234 pages. 2007.

Vol. 4505: G. Dong, X. Lin, W. Wang, Y. Yang, J.X. Yu (Eds.), Advances in Data and Web Management. XXII, 896 pages. 2007.

Vol. 4504: J. Huang, R. Kowalczyk, Z. Maamar, D. Martin, I. Müller, S. Stoutenburg, K.P. Sycara (Eds.), Service-Oriented Computing: Agents, Semantics, and Engineering. X, 175 pages. 2007.

Vol. 4501: J. Marques-Silva, K.A. Sakallah (Eds.), Theory and Applications of Satisfiability Testing – SAT 2007. XI, 384 pages. 2007.

Vol. 4500: N. Streitz, A. Kameas, I. Mavrommati (Eds.), The Disappearing Computer. XVIII, 304 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4498: N. Abdennadher, F. Kordon (Eds.), Reliable Software Technologies – Ada Europe 2007. XIV, 247 pages. 2007.

Vol. 4497: S.B. Cooper, B. Löwe, A. Sorbi (Eds.), Computation and Logic in the Real World. XVIII, 826 pages. 2007.

Vol. 4496: N.T. Nguyen, A. Grzech, R.J. Howlett, L.C. Jain (Eds.), Agent and Multi-Agent Systems: Technologies and Applications. XXI, 1046 pages. 2007. (Sublibrary LNAI).

Vol. 4495: J. Krogstie, A. Opdahl, G. Sindre (Eds.), Advanced Information Systems Engineering. XVI, 606 pages. 2007.

Vol. 4494: H. Jin, O.F. Rana, Y. Pan, V.K. Prasanna (Eds.), Algorithms and Architectures for Parallel Processing. XIV, 508 pages. 2007.

Vol. 4493: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part III. XXVI, 1215 pages. 2007.

Vol. 4492: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part II. XXVII, 1321 pages. 2007.

Vol. 4491: D. Liu, S. Fei, Z.-G. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part I. LIV, 1365 pages. 2007.

Vol. 4490: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part IV. XXXVII, 1211 pages. 2007.

Vol. 4489: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part III. XXXVII, 1257 pages. 2007.

Vol. 4488: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part II. XXXV, 1251 pages. 2007.

Vol. 4487: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part I. LXXXI, 1275 pages. 2007.

Vol. 4486: M. Bernardo, J. Hillston (Eds.), Formal Methods for Performance Evaluation. VII, 469 pages. 2007.

Vol. 4485: F. Sgallari, A. Murli, N. Paragios (Eds.), Scale Space and Variational Methods in Computer Vision. XV, 931 pages. 2007.

Vol. 4484: J.-Y. Cai, S.B. Cooper, H. Zhu (Eds.), Theory and Applications of Models of Computation. XIII, 772 pages. 2007.

Vol. 4483: C. Baral, G. Brewka, J. Schlipf (Eds.), Logic Programming and Nonmonotonic Reasoning. IX, 327 pages. 2007. (Sublibrary LNAI).

Vol. 4482: A. An, J. Stefanowski, S. Ramanna, C.J. Butz, W. Pedrycz, G. Wang (Eds.), Rough Sets, Fuzzy Sets, Data Mining and Granular Computing. XIV, 585 pages. 2007. (Sublibrary LNAI).

Vol. 4481: J. Yao, P. Lingras, W.-Z. Wu, M. Szczuka, N.J. Cercone, D. Ślęzak (Eds.), Rough Sets and Knowledge Technology. XIV, 576 pages. 2007. (Sublibrary LNAI).

Vol. 4480: A. LaMarca, M. Langheinrich, K.N. Truong (Eds.), Pervasive Computing. XIII, 369 pages. 2007.

Vol. 4479: I.F. Akyildiz, R. Sivakumar, E. Ekici, J.C.d. Oliveira, J. McNair (Eds.), NETWORKING 2007. Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. XXVII, 1252 pages. 2007.

Vol. 4478: J. Martí, J.M. Benedí, A.M. Mendonça, J. Serrat (Eds.), Pattern Recognition and Image Analysis, Part II. XXVII, 657 pages. 2007.

Vol. 4477: J. Martí, J.M. Benedí, A.M. Mendonça, J. Serrat (Eds.), Pattern Recognition and Image Analysis, Part I. XXVII, 625 pages. 2007.

Vol. 4476: V. Gorodetsky, C. Zhang, V.A. Skormin, L. Cao (Eds.), Autonomous Intelligent Systems: Multi-Agents and Data Mining. XIII, 323 pages. 2007. (Sublibrary LNAI).

Vol. 4475: P. Crescenzi, G. Prencipe, G. Pucci (Eds.), Fun with Algorithms. X, 273 pages. 2007.

Vol. 4474: G. Prencipe, S. Zaks (Eds.), Structural Information and Communication Complexity. XI, 342 pages. 2007.

Vol. 4472: M. Haindl, J. Kittler, F. Roli (Eds.), Multiple Classifier Systems. XI, 524 pages. 2007.

¥484.00元

Table of Contents

Real-Time Utilities for Ada 2005*

Andy Wellings and Alan Burns

Department of Computer Science, University of York, UK
{andy,burns}@cs.york.ac.uk

Abstract. Modern large real-time systems are becoming more complex. Whilst Ada 2005 provides a comprehensive set of programming mechanisms that allow these systems to be implemented, the abstractions are low level. This paper argues that there is a need for a standardised library of real-time utilities that address common real-time problems. The paper presents some initial considerations on what could be in such a library and how it could be structured.

1 Introduction

Ada has comprehensive support for priority-based real-time systems. The approach has been to provide a set of low-level mechanisms that enable the programmer to construct systems solving common real-time problems. Whilst eminently flexible, this approach requires the programmer to re-implement common paradigms in each new system. In the past, these structures have been quite straightforward, perhaps just involving simply periodic or sporadic tasks communicating via protected data. However, modern large real-time systems are much more complex and include hard, soft and non real-time components. The resulting paradigms are similarly more involved, and require activities like deadline miss detection, CPU budget overrun detection, the sharing of CPU budgets between aperiodic threads etc. Ada 2005 has responded admirably, expanding its set of low-level mechanisms. However, the common problems are now much more complex, and it is no longer appropriate to require the programmer to reconstruct the algorithms in each new system. Instead, what is required is a library of reusable real-time utilities; indeed, ideally such a library should become a de facto secondary standard – perhaps in the same way that Java has developed a set of concurrency utilities over the years that have now been incorporated into the Java 1.5 distribution.

The goal of this paper is to initiate a discussion in the Ada community to both confirm the need for a library of common real-time utilities and to propose (as a starting point) a framework for their construction.

2 Real-Time Utilities – Framework Overview

In the field of real-time programming, real-time tasks are often classified as being periodic, sporadic or aperiodic. Simple real-time periodic tasks are easy to program but

* This work has been undertaken within the context of the EU ARTIST2 project.

N. Abdennahder, F. Kordon (Eds.): Ada-Europe 2007, LNCS 4498, pp. 1–14, 2007.

once more complicated ones are needed (such as those that detect deadline misses, execution time (budget) overruns, minimum inter-arrival violations etc), the paradigms become more complex. Hence, there is a need to package up some of these and provide them as real-time tasking utilities.

A programmer wanting to use a real-time tasking abstraction will want to indicate (for example):

- whether the abstraction is periodic, sporadic or aperiodic (each task is "released" in response to a release event, which is usually time triggered for periodic tasks and event triggered for sporadic and aperiodic tasks);
- whether to terminate the current release of the task in the event of a deadline miss or to simply inform the program that this event has occurred (in which case, the programmer can choose to react or ignore the event);
- whether to terminate the current release of the task in the event of an execution time overrun or to simply inform the program that this event has occurred (in which case, the program can choose to react or ignore the event);
- whether a task is associated with an execution-time server that can limit the amount of CPU-time it receives.
- whether a task can operate in one or more modes, and if so, the nature of the mode change.

This paper illustrates how real-time task abstractions, supporting some of these variations, can be developed in Ada 2005. The approach that has been taken is to divide the support for the tasks into four components.

1. The functionality of the task – this is encapsulated by the `Real_Time_Task_State` package. Its goal is to define a structure for the application code of the tasks. It is here that code is provided: to execute on each release of the task, to execute when deadline misses occur and when execution time overruns occurs. In this paper, it is assumed that the task only wishes to operate in a single mode.
2. The mechanisms needed to control the release of the real-time tasks and to detect the deadline misses and execution time overruns – this is encapsulated in the `Release_Mechanisms` package. Each mechanism is implemented using a combinations of protected objects and the new Ada 2005 timer and execution time control features.
3. The various idioms of how the task should respond to deadline misses and execution time overruns – this is encapsulated in the `Real_Time_Task` package. It is here that the actual Ada tasks are provided.
4. The mechanisms needed to encapsulate subsystems and ensure that they are only given a fixed amount of the CPU resource (often called temporal firewalling) – this is the responsibility of the `Execution_Servers` package. This paper considers using these mechanisms to support aperiodic task execution only.

Figure 1 illustrates the top level packages that make up the abstractions. The details are discussed in the following sections.

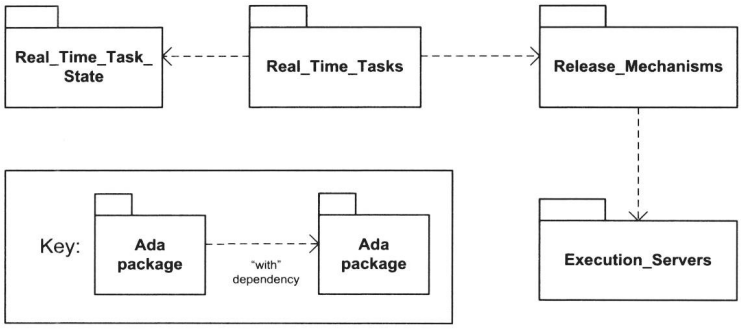

Fig. 1. Top-Level Packages

3 Framework Design

This section describes the details of the design of the framework introduced in Section 2. It assumes fixed priority scheduling and that the deadlines of all periodic tasks are less than or equal to their associated periods.

3.1 Real-Time Task State

First, it is necessary to provide a structure within which the programmer can express the code that the real-time task wishes to execute, along with its associated state variables. This is achieved, in the usual Ada object-oriented fashion, by defining the state within a tagged type, and providing operations to execute on the state. The following package shows the state and operations that all real-time tasks need.

```
-- with and use clauses omitted
package Real_Time_Task_State is
  type Task_State is abstract tagged record
    Relative_Deadline : Time_Span := Time_Span_Last;
    Execution_Time : Time_Span := Time_Span_Last;
    Pri : Priority := Default_Priority;
  end record;
  procedure Initialize(S: in out Task_State) is abstract;
  procedure Code(S: in out Task_State) is abstract;
  procedure Deadline_Miss(S: in out Task_State) is null;
  procedure Overrun(S: in out Task_State) is null;
  type Any_Task_State is access all Task_State'Class;
end Real_Time_Task_State;
```

Every real-time task has a deadline, an execution time and a priority. Here, these fields are made public, but they could have just as well been made private and procedures to 'get' and 'set' them provided. No additional assumptions have been made about the values of these attributes. The operations to be performed on a task's state are given by four procedures:

- `Initialize`: this is used to initialize the state when the real-time task is created;
- `Code`: – this is the code that is executed on each release of the task;