Lecture Notes in Computer Science 4745

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

Emmanuel Gaudin Elie Najm Rick Reed (Eds.)

SDL 2007: Design for Dependable Systems

13th International SDL Forum
Paris, France, September 18-21, 2007
Proceedings

Springer

Volume Editors

Emmanuel Gaudin
PragmaDev SARL
18, rue des Tournelles, 75004 Paris, France
E-mail: emmanuel.gaudin@pragmadev.com

Elie Najm
ENST
Département Informatique et Réseaux
46, rue Barrault, 75634 Paris Cedex 13, France
E-mail: Elie.Najm@ENST.fr

Rick Reed
Telecommunications Software Engineering Limited
The Laurels, Victoria Road, Windermere, Cumbria LA23 2DL, United Kingdom
E-mail: rickreed@tseng.co.uk

Library of Congress Control Number: 2007934912

CR Subject Classification (1998): C.2, D.2, D.3, F.3, C.3, H.4

LNCS Sublibrary: SL 5 – Computer Communication Networks and Telecommunications

ISSN 0302-9743
ISBN-10 3-540-74983-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74983-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12161393 06/3180 5 4 3 2 1 0

Preface

This volume contains the papers presented at the 13^{th} SDL Forum, Paris, France entitled "Design for Dependable Systems" and reflects the intent to have a balance between experience reports and research papers related to System Design Languages.

The language that was at the heart of the first few SDL Forums was the ITU-T Specification and Description Language defined in Z.100, and the application domain was almost entirely fixed-line telephone communication. Mobile telephony was for the super-rich and electronics in cars was just for radios.

Ever since its inception, 30 years ago, the Z.100 language has been used for model-driven development in the telecommunication industry. Nowadays, model-driven engineering is a must for all industries and has been generalized by OMG to all application domains as covered by a paper on an automotive case study in this volume. What has been happening over the past few years is that the infrastructure has been put in place providing good support for the model-driven paradigm, so that the economic benefit of the approach makes it more of a necessity than a choice for designing dependable systems. The experience report from Motorola in this volume underlines this trend.

Although the SDL Forum Society that organizes these SDL Forums has it roots in telecommunications, the System Design Languages needed for modeling in that industry are applied in other real-time engineering domains such as aerospace, the ubiquitous Bluetooth devices, and railways. For the last few years all modeling languages and technologies have had a tendency to converge towards UML, and since UML 2.0 and its profile definition capability came out, there is now an amazing number of diverging profile proposals based on older technologies. This was reflected in the conference programme with tutorials on SysML, SDL-RT, MARTE, and Z.109 covering different aspects of system modeling. An example in this volume is the paper that utilizes the UML 2.0 Testing Profile.

This latter paper is one of a number that shows the continuing interest and developments in the ITU-T Testing and Test Control Notation (TTCN). Although much of the evolution of TTCN has been through the work of ETSI, it is still largely seen as an ITU-T standard. In some ways this makes sense as ITU-T re-publishes the ETSI revisions of TTCN as a truly international standard (Z.140 series). TTCN is widely used with the ITU-T Message Sequence Chart (Z.120) and Specification and Description Language (Z.100 series). These are also used with another ITU-T product, Abstract Syntax Notation One (X.680 series), which is used to define protocol data units with their associated encoding rules (X.690 series). However, these languages are not thought to be adequate to capture requirements. A new language for User Requirements Notation (Z.150 series) is in progress, which includes Use Case Maps — covered by another paper in this volume.

So with all these ITU-T languages for system design, what is the role of UML?

UML is seen, as its name implies, as a unifying concept between languages. Because UML leaves a number a semantic issues open and even states frequently that there is *no specific notation* for a particular concept, it is in reality largely a framework that has to be populated with specific semantics and notations before it can be used to completely develop products. One route is to choose a particular UML tool, whose implementation (such as writing actions in C or Java) will have fixed certain issues, but at the cost of potentially being locked into that tool. Another route is to provide UML profiles for existing languages, thus not only binding UML to the semantics and notation of the language, but also providing some glue between different notations. It is the latter route that the ITU-T is taking (albeit rather slowly), with Z.109 being approved in 2007 as the UML profile for Z.100. Other profiles are in the ITU-T work plan for X.680, Z.120, Z.140 and Z.150. A related path is presented in the first paper in the volume, providing a meta-model for (a subset of) Z.100.

UML also has another role. If you ask someone who claims to be using UML which diagrams they use, often the reply will be that they mainly use Class Diagrams and Object Diagrams. The other 11 types of UML diagrams are used less frequently and some quite rarely (if at all). This is partly because the Class Diagrams and Object Diagrams meet a need that is not well met by other notations. Even the ITU-T in its 1996 Z.100 SDL+ methodology supplement suggested using diagrams in the Object-Modeling Technique notation (a forerunner of UML subsumed into UML in the unifying process). This is why it is natural to use these diagrams with the ITU-T languages: UML is frequently used for class and object modeling with Z.100 and other state machine languages in this volume and elsewhere. UML therefore not only provides the glue, but itself provides an important member of a set of System Design Languages.

Although the original Z.100 of 30 years ago was a paper and pencil language, none of this engineering today would be practical without computer-based tools because the systems in question are much more complex. This is evident from most of papers. As well as tools to directly support System Design Languages, included in this volume are papers on a real-time operating system and the use of probability modeling to analyze realistic-size networks without encountering state space explosion. At first glance, it may seem that these papers are not relevant, but you will probably change your mind when you read the papers, as a key issue in both cases is performance. There are many factors involved in the design for dependable real-time systems, so it is hard to predict what might be relevant for a future SDL Forum.

Thanks

A volume such as this could not, of course, exist without the contributions of the authors, who are thanked for their work.

The Programme Committee were also the reviewers of the papers, and are thanked for their work selecting the papers and the programme.

Irfan Hamid of ENST is thanked for his editorial assistance in preparing this volume.

The organization was greatly assisted by the various sponsors that provided valuable support. SDL 2007 was sponsored by:

- Centre National de la Recherche Scientifique
- Cinderella
- France Telecom
- PragmaDev
- Télécom Paris - École Nationale Supérieure des Télécommunications (ENST)
- Telelogic

July 2007

Emmanuel Gaudin
Elie Najm
Rick Reed

Organization

Each SDL Forum is organized by the SDL Forum Society with the help of local organizers. The Organizing Committee consists of the Board of the SDL Forum Society plus the local organizers and others as needed depending on the actual event. For SDL 2007 the local organizers from PragmaDev and ENST need to be thanked for their effort to ensure that everything was in place for the presentation of the papers in this volume.

Organizing Committee

Chairman, SDL Forum Society	Rick Reed (TSE Ltd.)
Treasurer, SDL Forum Society	Martin von Löwis (Hasso-Plattner-Institut)
Secretary, SDL Forum Society	Andreas Prinz (Agder University College)
Conference Chair	Emmanuel Gaudin (PragmaDev)
Programme Committee Chair	Elie Najm (ENST)

Programme Committee

Daniel Amyot (Université d'Ottawa, Canada)
Reibert Arbring (Ericsson, Sweden)
Rolv Bræk (NTNU, Norway)
Eric Brunel (PragmaDev, France)
Pierre Combes (France Telecom, France)
Philippe Desfray (Objecteering Software, France)
Laurent Doldi (Isoscope, France)
Anders Ek (Telelogic, Sweden)
Jaqueline Floch (SINTEF, Norway)
Birgit Geppert (Avaya Labs Research, USA)
Reinhard Gotzhein (Universität Kaiserslautern, Germany)
Jens Grabowski (University of Göttingen, Germany)
Susanne Graf (Verimag, France)
Peter Graubmann (Siemens, Germany)
Loïc Hélouët (INRIA Rennes, France)
Paul Herber (Sandrila, UK)
Dieter Hogrefe (ETSI - MTS, Germany)
Eckhardt Holz (University of Potsdam, Germany)
Ferhat Khendek (Concordia University, Canada)
Tae-Hyong, Kim, KIT, Korea)
Shashi Kumar (Jönköping University, Sweden)
Philippe Leblanc (Telelogic, France)

Vesa Luukkala (Nokia, Finland)
Anna Medve (University of Pannonia, Hungary)
Pedro Merino Gómez (University of Malaga, Spain)
François Michaillat (Alcatel, France)
Birger Møller-Pedersen (University of Oslo, Norway)
Elie Najm (ENST Paris, France)
Patrik Nandorf (Ericsson, Sweden)
Ian Oliver (Nokia, Finland)
Anders Olsen (Cinderella, Denmark)
Benoit Parreaux (France Telecom, France)
Javier Poncela González (University of Malaga, Spain)
Andreas Prinz (Agder University College, Norway)
Rick Reed (TSE, UK)
Manuel Rodríguez Cayetano (University of Valladolid, Spain)
Eldor Rødseth (SystemSoft, Norway)
Alain Rossignol (Astrium, France)
Richard Sanders (SINTEF, Norway)
Amardeo Sarma (NEC, Germany)
Ina Schieferdecker (Fraunhofer FOKUS, Germany)
Bran Selic (IBM Rational, Canada)
Edel Sherratt (University of Wales Aberystwyth, UK)
Martin von Löwis (Hasso-Plattner-Institut Potsdam, Germany)
Thomas Weigert (Motorola, USA)

SDL Forum Society

The SDL Forum Society is a not-for-profit organization that in addition to running the SDL Forum:

- Runs the SAM (System Analysis and Modeling) workshop every 2 years between SDL Forum years.
- Is a body recognized by ITU-T as co-developing the Z.100 to Z.109 and Z.120 to Z.129 and other language standards;
- Promotes the ITU-T System Design Languages.

For more information on the SDL Forum Society, see `www.sdl-forum.org`.

Table of Contents

Model Driven Engineering

Testing

Language Extensions

Implementation

Modeling Experience and Extensions