Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

387

C. Ghezzi J.A. McDermid (Eds.)

ESEC '89

2nd European Software Engineering Conference
University of Warwick, Coventry, UK
September 11–15, 1989
Proceedings

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo Hong Kong

Editors

Carlo Ghezzi
Dipartimento di Elettronica, Politecnico di Milano
Piazza Leonardo Da Vinci 32, I-20133 Milano, Italia

John A. McDermid
Department of Computer Science, University of York
York YO1 5DD, UK

CR Subject Classification (1987): D.2

ISBN 3-540-51635-2 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-51635-2 Springer-Verlag New York Berlin Heidelberg

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2146/3140-543210 – Printed on acid-free paper

Preface

The term "Software Engineering" was first introduced at a NATO conference held in Garmisch Partenkirchen in 1968. Since then there has been a large amount of high quality software engineering research and development carried out in Europe. With the advent of the ESPRIT program the volume and quality of work, especially that carried out on an international collaborative basis, has increased dramatically. However there has not been a natural forum for discussing the results of this, and other European work, so in 1986 the major European computer and informatics societies agreed to set up a series of software engineering conferences. The series of European Software Engineering Conferences, or ESEC, started in Strasbourg in 1987. The second conference in the series, ESEC '89, was arranged for Warwick in the UK, in September 1989.

Although the conference is intended primarily as a forum for discussion of research and current practice in software engineering within Europe, the conference is not restricted to European participation or papers. Indeed the 1989 conference includes presentations from the United States and Australasia, as well as most of the major countries of Europe. Thus the intention is that, although the ESEC conferences should be held in Europe, they should represent world class research and development activities.

ESEC is intended to be a meeting place for software engineers: it welcomes participants and contributions from all over the world, both from industry and academia, on both practical and theoretical aspects relating to software engineering. The conference, and hence these proceedings, cover a broad range of themes. Papers span a range from formal methods to their practical application, from measurements that can be applied to assess the quality of software processes and products to tools and environments supporting software production, from methods supporting production of reliable software to the principles of human computer interaction.

However it is not only the breadth of coverage that characterises ESEC '89. Quality and depth of papers is the other important aspect. Every paper in this volume is characterised by either new and promising ideas or by new and deep insights into known concepts. Along with an excellent selection of contributed papers, we are proud to present a number of invited papers written by experts who are internationally recognised in their particular fields of interest. We are sure that the blending of all these ingredients results in a stimulating conference programme and that the papers collected in this volume will be seen as an important contribution to the field by the software engineering community.

Since it is now 21 years since the term "Software Engineering" was introduced it might be nice to think that software engineering has now "come of age". However it seems that there are many areas of our discipline where we still do not have an adequate set of principles and techniques for addressing particular problems. Also there are many cases where techniques that have been developed in research laboratories have yet to be put into industrial practice. Consequently there is still a necessity for a forum for discussing research results, for trying to transfer technology from research into application, and for hearing results of practical applications of advanced techniques in order that future research can be informed by the success, or otherwise, of current techniques when put into practice. We hope that the ESEC series of conferences will continue to fill this role.

Finally we would like to acknowledge the help in organising this conference from the Programme Committee. Thanks to the enthusiastic support of all members of the Programme Committee, we have been able to put together a set of outstanding papers that reflect the state of the art in software engineering research, and practice, and that will contribute greatly to the advances of software engineering.

Carlo Ghezzi, Programme Committee Chairman
John McDermid, Conference Chairman

Contents

Keynote Paper

Software risk management 1
B. Boehm

Invited Papers

MENU - An example for the systematic reuse of specifications 20
M. Wirsing, R. Hennicker and R. Stabl

Asking for the impossible : The state of the art in safety-related systems 42
M. Thomas

STEPS to software development with users 48
C. Floyd, F.-M. Reisin and G. Schmidt

Measurement

The role of measurement in ISEEs 65
H. D. Rombach

An empirical and theoretical analysis of an information flow-based system design metric 86
D. C. Ince and M. J. Shepperd

Software Processes Modelling

Systematic development of formal software process models 100
W. Deiters, W. Schaefer and V. Gruhn

Software process machines : a framework for future software development environments 118
P. Armenise

Practical Experience with Formal Methods

Practical experience of formal specification : a programming interface for communications 140
J. Wordsworth

Industrialising formal methods for telecommunications 159
M. T. Norris and S. G. Stockman

Software Configuration Management

An application of the event calculus for representing the history of a software project 176
D. Nardi and M. Tucci

Change oriented versioning 191
A. Lie, T. Didriksen, R. Conradi and E.-A. Karlsson, S. O. Hallsteinsen and P. Holager

Software change dynamics or half of all Ada™ compilations are redundant 203
R. Adams, A. Weinert and W .Tichy

Version management in the PACT integrated software engineering environment 222
F. Oquendo, K. Berrada, F. Gallo, R. Minot and I. Thomas

Formal Approaches

Software engineering implications for formal refinement 243
A. Dix

A rigorous development strategy using the OBJ specification language and the MALPAS program analysis tool 260
R. N. Shutt

Formal specification using structured systems analysis 292
R. B. France and T. W. G. Docker

Tools and Environments

Tool integration in an open environment 311
M. Lacroix and M. Vanhoedenaghe

HCDM/GSDS - A design environment for real-time software with automatic program generation 324
M. Fastenbauer and H. Saria

Graph grammars, a new paradigm for implementing visual languages 336
H. Goettler

Software Metrics

Structural modelling of prolog for metrication 351
M. Myers

Rule-based handling of software quality and productivity models 376
H.-L. Hausen

Requirements Engineering

An object-oriented approach to the system analysis 395
F. Manfredi, G. Orlando and P. Tortorici

A pluralistic knowledge-based approach to software specification 411
C. Niskier, T. Maibaum and D. Schwabe

PROTOB : a hierarchical object-oriented CASE tool for distributed systems 424
M. Baldassari, G. Bruno, V. Russi and R. Zompi

Analysis and Validation

The internet worm incident 446
E. H. Spafford

Validation of concurrent Ada™ programs using symbolic execution 469
S. Morasca and M. Pezze

Assay - a tool to support regression testing 487
R. Lewis, D. W. Beck and J. Hartmann