Rune Winther
Bjørn Axel Gran
Gustav Dahll (Eds.)

Computer Safety, Reliability, and Security

LNCS 3688

24th International Conference, SAFECOMP 2005
Fredrikstad, Norway, September 2005
Proceedings

Springer

Rune Winther Bjørn Axel Gran
Gustav Dahll (Eds.)

Computer Safety, Reliability, and Security

24th International Conference, SAFECOMP 2005
Fredrikstad, Norway, September 28-30, 2005
Proceedings

Springer

Volume Editors

Rune Winther
Østfold University College
Faculty of Computer Sciences
1757 Halden, Norway
E-mail: rune.winther@hiof.no

Bjørn Axel Gran
Gustav Dahll
Institute for Energy Technology
Software Engineering Laboratory
1761 Halden, Norway
E-mail: bjorn.axel.gran@hrp.no; g.dahll@halden.net

Library of Congress Control Number: 2005932842

CR Subject Classification (1998): D.1-4, E.4, C.3, F.3, K.6.5

ISSN 0302-9743
ISBN-10 3-540-29200-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-29200-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11563228 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3688

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

Editorial Board

Preface

Welcome to SAFECOMP 2005, held in Fredrikstad, Norway. Since its establishment SAFECOMP, the series of conferences on Computer Safety, Reliability and Security, has contributed to the progress of the state of the art in dependable applications of computer systems. SAFECOMP provides ample opportunity to exchange insights and experiences in emerging methods and practical experience across the borders of different disciplines. Previous SAFECOMPs have year after year registered new multidisciplinary trends on dependability of computer-based systems.

SAFECOMP 2005 focused on dependability of critical computer applications and was a platform for knowledge and technology transfer between academia, industry and research institutions. Papers were invited on all aspects of dependability and survivability of critical computer-based systems in various branches and infrastructures. Due to the increasing awareness and importance of security issues of critical computer-based systems, SAFECOMP 2005 emphasized work in this area. Nowadays practical experience points out the need for multidisciplinary approaches to deal with the nature of critical complex settings.

The SAFECOMP 2005 program consisted of 30 papers selected from 84 submissions. The 30 papers represented scientists from 14 different countries acknowledging the world-wide interest of SAFECOMP and the addressed topics. The SAFECOMP program was supplemented by keynote talks enhancing the technical and scientific merit of the conference, a number of co-located activities, meetings and tutorials, and a technical visit to the research environment in Halden which organized the conference.

We would like to thank the International Program Committee, the external reviewers, the keynote speakers, and the authors for their work in support of SAFECOMP 2005. We would also like to thank the conference staff at the Institute of Energy Technology and Østfold University College. We really enjoyed the work, and we hope you appreciated the care we put into organizing the conference. Finally, we would like to extend to you the invitation to attend and contribute to SAFECOMP 2006 in Gdansk, Poland (www.safecomp.org).

July 2005

Gustav Dahll
Bjørn Axel Gran
Rune Winther

Organization

SAFECOMP 2005 Organization

General Chair

Gustav Dahll, Norway

Program Co-chairs

Bjørn Axel Gran, Norway
Rune Winther, Norway

EWICS Chair

Udo Voges, Germany

Organizing Committee

Rune Fredriksen, Norway
Siv-Hilde Houmb, Norway
Monica Kristiansen, Norway
John Petter Kvalvik, Norway
Jørn L. Pettersen, Norway
Atoosa P.-J. Thunem, Norway
Bjørn Axel Gran, Norway
Rune Winther, Norway

Institute for Energy Technology

International Program Committee

Stuart Anderson, UK
Terje Aven, Norway
Ramesh Bharadwaj, USA
Robin Bloomfield, UK
Sandro Bologna, Italy
Andrea Bondavalli, Italy
Inga-Lill Bratteby-Ribbing, Sweden
Bettina Buth, Germany
Stefan Christiernin, Sweden
Gustav Dahll, Norway
Peter Daniel, UK
Massimo Felici, UK
Robert Genser, Austria
Chris Goring, UK
Januscz Gorski, Poland
Bjorn Axel Gran, Norway
Wolfgang Grieskamp, USA
Wolfgang Halang, Germany
Kai Hansen, Norway
Monika Heiner, Germany
Maritta Heisel, Germany
Connie Heitmeyer, USA
Atte Helminen, Finland
Peter Jacobsson, Sweden
Ole-Arnt Johnsen, Norway
Chris Johnson, UK
Erland E. Jonsson, Sweden
Mohamed Kaâniche, France
Karama Kanoun, France
Martin Kropic, Czech Republic
Kenneth Kvinnesland, Norway
Dennis Kügler, Germany
Peter B. Ladkin, Germany
Peter Liggesmeyer, Germany
Oliver Mäckel, Germany
Meine van der Meulen, UK
Odd Nordland, Norway
Jan G. Nordstrøm, Norway
Alberto Pasquini, Italy
Gerd Rabe, Germany
Felix Redmill, UK
Judith Rossebø, Norway
Martin Rothfelder, Germany
Francesca Saglietti, Germany
Erwin Schoitsch, Austria
Terje Sivertsen, Norway
Jeanine Souquières, France
Werner Stephan, Germany
Ketil Stølen, Norway
Tor Stålhane, Norway
Asuman Suenbuel, USA
Mark Sujan, UK
Thomas Santen, Germany
Atoosa P.-J. Thunem, Norway
Jos Trienekens, The Netherlands
Adolfo Villafiorita, Italy
Udo Voges, Germany
Albrecht Weinert, Germany
Marc Wilikens, Italy
Rune Winther, Norway
Stefan Wittmann, Germany
Eric Wong, USA
Zdzislaw Zurakowski, Poland

External Reviewers

Matthias Anlauff
Terje Andersen
Lassaad Cheikhrouhou
Silvano Chiaradonna
Felicita Di Giandomenico
Lorenzo Falai
Siv-Hilde Houmb
Martin Gilje Jaatun
Terje Jensen
Tor Hjalmar Johannessen
Mass Soldal Lund
Tom Lysemose
Andreas Nonnengart
Simone Pozzi
Yu Qi
Atle Refsdal
Georg Rock
Luca Save
Fredrik Seehusen
Nikolai Tillmann
Inger Anne Tøndel
Fredrik Vraalsen
Linzhang Wang

Sponsoring Organizations

Scientific Sponsor

Scientific Co-sponsors

IFIP WG10.4 on Dependable Computing and Fault Tolerance
IFIP WG13.5 on Human Error, Safety and System Development

European
Network of
Clubs for
REliability and
Safety of
Software

Halden IT Forum
SCSC - Safety-Critical Systems Club
SRMC - Software Reliability & Metrics Club
NONSTOPP - NOrsk Nettverk for Sikre Trygge Og Pålitelige Programmerbare Systemer

Lecture Notes in Computer Science

For information about Vols. 1–3631

please contact your bookseller or Springer

Vol. 3738: V.R. Syrotiuk, E. Chávez (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XI, 360 pages. 2005.

Vol. 3728: V. Paliouras, J. Vounckx, D. Verkest (Eds.), Integrated Circuit and System Design. XV, 753 pages. 2005.

Vol. 3726: L.T. Yang, O.F. Rana, B. Di Martino, J. Dongarra (Eds.), High Performance Computing and Communcations. XXVI, 1116 pages. 2005.

Vol. 3725: D. Borrione, W. Paul (Eds.), Correct Hardware Design and Verification Methods. XII, 412 pages. 2005.

Vol. 3724: P. Fraigniaud (Ed.), Distributed Computing. XIV, 520 pages. 2005.

Vol. 3718: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing. XII, 502 pages. 2005.

Vol. 3717: B. Gramlich (Ed.), Frontiers of Combining Systems. X, 321 pages. 2005. (Subseries LNAI).

Vol. 3715: E. Dawson, S. Vaudenay (Eds.), Progress in Cryptology – Mycrypt 2005. XI, 329 pages. 2005.

Vol. 3714: H. Obbink, K. Pohl (Eds.), Software Product Lines. XIII, 235 pages. 2005.

Vol. 3713: L. Briand, C. Williams (Eds.), Model Driven Engineering Languages and Systems. XV, 722 pages. 2005.

Vol. 3712: R. Reussner, J. Mayer, J.A. Stafford, S. Overhage, S. Becker, P.J. Schroeder (Eds.), Quality of Software Architectures and Software Quality. XIII, 289 pages. 2005.

Vol. 3711: F. Kishino, Y. Kitamura, H. Kato, N. Nagata (Eds.), Entertainment Computing - ICEC 2005. XXIV, 540 pages. 2005.

Vol. 3710: M. Barni, I. Cox, T. Kalker, H.J. Kim (Eds.), Digital Watermarking. XII, 485 pages. 2005.

Vol. 3708: J. Blanc-Talon, W. Philips, D. Popescu, P. Scheunders (Eds.), Advanced Concepts for Intelligent Vision Systems. XXII, 725 pages. 2005.

Vol. 3707: D.A. Peled, Y.-K. Tsay (Eds.), Automated Technology for Verification and Analysis. XII, 506 pages. 2005.

Vol. 3706: H. Fuks, S. Lukosch, A.C. Salgado (Eds.), Groupware: Design, Implementation, and Use. XII, 378 pages. 2005.

Vol. 3703: F. Fages, S. Soliman (Eds.), Principles and Practice of Semantic Web Reasoning. VIII, 163 pages. 2005.

Vol. 3702: B. Beckert (Ed.), Automated Reasoning with Analytic Tableaux and Related Methods. XIII, 343 pages. 2005. (Subseries LNAI).

Vol. 3699: C.S. Calude, M.J. Dinneen, G. Păun, M. J. Pérez-Jiménez, G. Rozenberg (Eds.), Unconventional Computation. XI, 267 pages. 2005.

Vol. 3698: U. Furbach (Ed.), KI 2005: Advances in Artificial Intelligence. XIII, 409 pages. 2005. (Subseries LNAI).

Vol. 3697: W. Duch, J. Kacprzyk, E. Oja, S. Zadrożny (Eds.), Artificial Neural Networks: Formal Models and Their Applications – ICANN 2005, Part II. XXXII, 1045 pages. 2005.

Vol. 3696: W. Duch, J. Kacprzyk, E. Oja, S. Zadrożny (Eds.), Artificial Neural Networks: Biological Inspirations – ICANN 2005, Part I. XXXI, 703 pages. 2005.

Vol. 3695: M.R. Berthold, R. Glen, K. Diederichs, O. Kohlbacher, I. Fischer (Eds.), Computational Life Sciences. XI, 277 pages. 2005. (Subseries LNBI).

Vol. 3694: M. Malek, E. Nett, N. Suri (Eds.), Service Availability. VIII, 213 pages. 2005.

Vol. 3693: A.G. Cohn, D.M. Mark (Eds.), Spatial Information Theory. XII, 493 pages. 2005.

Vol. 3692: R. Casadio, G. Myers (Eds.), Algorithms in Bioinformatics. X, 436 pages. 2005. (Subseries LNBI).

Vol. 3691: A. Gagalowicz, W. Philips (Eds.), Computer Analysis of Images and Patterns. XIX, 865 pages. 2005.

Vol. 3690: M. Pěchouček, P. Petta, L.Z. Varga (Eds.), Multi-Agent Systems and Applications IV. XVII, 667 pages. 2005. (Subseries LNAI).

Vol. 3688: R. Winther, B.A. Gran, G. Dahll (Eds.), Computer Safety, Reliability, and Security. XIII, 405 pages. 2005.

Vol. 3687: S. Singh, M. Singh, C. Apte, P. Perner (Eds.), Pattern Recognition and Image Analysis, Part II. XXV, 809 pages. 2005.

Vol. 3686: S. Singh, M. Singh, C. Apte, P. Perner (Eds.), Pattern Recognition and Data Mining, Part I. XXVI, 689 pages. 2005.

Vol. 3685: V. Gorodetsky, I. Kotenko, V. Skormin (Eds.), Computer Network Security. XIV, 480 pages. 2005.

Vol. 3684: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part IV. LXXIX, 933 pages. 2005. (Subseries LNAI).

Vol. 3683: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. LXXX, 1397 pages. 2005. (Subseries LNAI).

Vol. 3682: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. LXXIX, 1371 pages. 2005. (Subseries LNAI).

Vol. 3681: R. Khosla, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXXX, 1319 pages. 2005. (Subseries LNAI).

Vol. 3679: S.d.C. di Vimercati, P. Syverson, D. Gollmann (Eds.), Computer Security – ESORICS 2005. XI, 509 pages. 2005.

Vol. 3678: A. McLysaght, D.H. Huson (Eds.), Comparative Genomics. VIII, 167 pages. 2005. (Subseries LNBI).

Vol. 3677: J. Dittmann, S. Katzenbeisser, A. Uhl (Eds.), Communications and Multimedia Security. XIII, 360 pages. 2005.

Vol. 3676: R. Glück, M. Lowry (Eds.), Generative Programming and Component Engineering. XI, 448 pages. 2005.

Vol. 3675: Y. Luo (Ed.), Cooperative Design, Visualization, and Engineering. XI, 264 pages. 2005.

Vol. 3674: W. Jonker, M. Petković (Eds.), Secure Data Management. X, 241 pages. 2005.

Vol. 3673: S. Bandini, S. Manzoni (Eds.), AI*IA 2005: Advances in Artificial Intelligence. XIV, 614 pages. 2005. (Subseries LNAI).

Vol. 3672: C. Hankin, I. Siveroni (Eds.), Static Analysis. X, 369 pages. 2005.

Vol. 3671: S. Bressan, S. Ceri, E. Hunt, Z.G. Ives, Z. Bellahsène, M. Rys, R. Unland (Eds.), Database and XML Technologies. X, 239 pages. 2005.

Vol. 3670: M. Bravetti, L. Kloul, G. Zavattaro (Eds.), Formal Techniques for Computer Systems and Business Processes. XIII, 349 pages. 2005.

Vol. 3669: G.S. Brodal, S. Leonardi (Eds.), Algorithms – ESA 2005. XVIII, 901 pages. 2005.

Vol. 3668: M. Gabbrielli, G. Gupta (Eds.), Logic Programming. XIV, 454 pages. 2005.

Vol. 3666: B.D. Martino, D. Kranzlmüller, J. Dongarra (Eds.), Recent Advances in Parallel Virtual Machine and Message Passing Interface. XVII, 546 pages. 2005.

Vol. 3665: K. S. Candan, A. Celentano (Eds.), Advances in Multimedia Information Systems. X, 221 pages. 2005.

Vol. 3664: C. Türker, M. Agosti, H.-J. Schek (Eds.), Peer-to-Peer, Grid, and Service-Orientation in Digital Library Architectures. X, 261 pages. 2005.

Vol. 3663: W.G. Kropatsch, R. Sablatnig, A. Hanbury (Eds.), Pattern Recognition. XIV, 512 pages. 2005.

Vol. 3662: C. Baral, G. Greco, N. Leone, G. Terracina (Eds.), Logic Programming and Nonmonotonic Reasoning. XIII, 454 pages. 2005. (Subseries LNAI).

Vol. 3661: T. Panayiotopoulos, J. Gratch, R. Aylett, D. Ballin, P. Olivier, T. Rist (Eds.), Intelligent Virtual Agents. XIII, 506 pages. 2005. (Subseries LNAI).

Vol. 3660: M. Beigl, S. Intille, J. Rekimoto, H. Tokuda (Eds.), UbiComp 2005: Ubiquitous Computing. XVII, 394 pages. 2005.

Vol. 3659: J.R. Rao, B. Sunar (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2005. XIV, 458 pages. 2005.

Vol. 3658: V. Matoušek, P. Mautner, T. Pavelka (Eds.), Text, Speech and Dialogue. XV, 460 pages. 2005. (Subseries LNAI).

Vol. 3657: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. VIII, 325 pages. 2005.

Vol. 3656: M. Kamel, A. Campilho (Eds.), Image Analysis and Recognition. XXIV, 1279 pages. 2005.

Vol. 3655: A. Aldini, R. Gorrieri, F. Martinelli (Eds.), Foundations of Security Analysis and Design III. VII, 273 pages. 2005.

Vol. 3654: S. Jajodia, D. Wijesekera (Eds.), Data and Applications Security XIX. X, 353 pages. 2005.

Vol. 3653: M. Abadi, L. de Alfaro (Eds.), CONCUR 2005 – Concurrency Theory. XIV, 578 pages. 2005.

Vol. 3652: A. Rauber, S. Christodoulakis, A M. Tjoa (Eds.), Research and Advanced Technology for Digital Libraries. XVIII, 545 pages. 2005.

Vol. 3651: R. Dale, K.-F. Wong, J. Su, O.Y. Kwong (Eds.), Natural Language Processing – IJCNLP 2005. XXI, 1031 pages. 2005. (Subseries LNAI).

Vol. 3650: J. Zhou, J. Lopez, R.H. Deng, F. Bao (Eds.), Information Security. XII, 516 pages. 2005.

Vol. 3649: W.M. P. van der Aalst, B. Benatallah, F. Casati, F. Curbera (Eds.), Business Process Management. XII, 472 pages. 2005.

Vol. 3648: J.C. Cunha, P.D. Medeiros (Eds.), Euro-Par 2005 Parallel Processing. XXXVI, 1299 pages. 2005.

Vol. 3646: A. F. Famili, J.N. Kok, J.M. Peña, A. Siebes, A. Feelders (Eds.), Advances in Intelligent Data Analysis VI. XIV, 522 pages. 2005.

Vol. 3645: D.-S. Huang, X.-P. Zhang, G.-B. Huang (Eds.), Advances in Intelligent Computing, Part II. XIII, 1010 pages. 2005.

Vol. 3644: D.-S. Huang, X.-P. Zhang, G.-B. Huang (Eds.), Advances in Intelligent Computing, Part I. XXVII, 1101 pages. 2005.

Vol. 3643: R. Moreno Díaz, F. Pichler, A. Quesada Arencibia (Eds.), Computer Aided Systems Theory – EUROCAST 2005. XIV, 629 pages. 2005.

Vol. 3642: D. Ślezak, J. Yao, J.F. Peters, W. Ziarko, X. Hu (Eds.), Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing, Part II. XXIII, 738 pages. 2005. (Subseries LNAI).

Vol. 3641: D. Ślezak, G. Wang, M. Szczuka, I. Düntsch, Y. Yao (Eds.), Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing, Part I. XXIV, 742 pages. 2005. (Subseries LNAI).

Vol. 3639: P. Godefroid (Ed.), Model Checking Software. XI, 289 pages. 2005.

Vol. 3638: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), Smart Graphics. XI, 269 pages. 2005.

Vol. 3637: J. M. Moreno, J. Madrenas, J. Cosp (Eds.), Evolvable Systems: From Biology to Hardware. XI, 227 pages. 2005.

Vol. 3636: M.J. Blesa, C. Blum, A. Roli, M. Sampels (Eds.), Hybrid Metaheuristics. XII, 155 pages. 2005.

Vol. 3634: L. Ong (Ed.), Computer Science Logic. XI, 567 pages. 2005.

Vol. 3633: C. Bauzer Medeiros, M. Egenhofer, E. Bertino (Eds.), Advances in Spatial and Temporal Databases. XIII, 433 pages. 2005.

Vol. 3632: R. Nieuwenhuis (Ed.), Automated Deduction – CADE-20. XIII, 459 pages. 2005. (Subseries LNAI).

Table of Contents

CMMI RAMS Extension Based on CENELEC Railway Standard

Jose Antonio Fonseca and Jorge Rady de Almeida Júnior

Computational and Digital Systems Engineering Department,
Polytechnic School, University of São Paulo, Brazil

Abstract. Railway systems are also dependable systems and, considering their importance, it is vital to assure the application of adequate design techniques. So, this work presents a RAMS (Reliability, Availability, Maintainability and Safety) extension for CMMI SE-SW version 1.1 "Capability Maturity Model® Integration" developed by SEI (Software Engineering Institute), based on CENELEC 50126, 50128 and 50129 standards developed to normalize RAMS aspects of railway control systems in European Community. This extension is based on the inclusion of four new Process Areas into the CMMI SE-SW, increasing its actual number from 22 to 26, without changes in the CMMI model basic structure. The objective of this extension is to obtain a support tool for design process applicable to enterprises that develop railway systems and are adopting CMMI or migrating from other CMM models.

1 Introduction

This work represents an attempt to join two very important tendencies that are being verified by the maturity models use and the railway applications design. Considering the great capacity of CMM models to assist innumerous application areas, the first trend can be observed through an increase in the use of maturity models by industrial community. The focus of such models is represented by CMMI (Capability Maturity Model Integration). The second trend is composed by integration efforts to create a consensus about RAMS (Reliability, Availability, Maintainability and Safety) criteria for railways applications between the European Union members that is represented by CENELEC standards.

This work has also a very closely relationship with others efforts to incorporate new specifics aspects to CMMI, such as the job sponsored by FAA (Federal Aviation Administration) to include Safety and Security requirements in iCMM and CMMI and the task headed by Australian Government's Defense Material Organization (DMO) in the creation of +Safe, a safety extension to CMMI.

The section 2 presents a brief description about the CMMI model, while section 3 presents the mains aspects of the CENELEC Standards. Section 4 contains the proposed extension of RAMS extension for CMMI model. Finally, section 5 presents the mains conclusions of this paper.

R. Winther, B.A. Gran, and G. Dahll (Eds.): SAFECOMP 2005, LNCS 3688, pp. 1 - 12, 2005.

2 The CMMI Model

The extensive use of the SW-CMM [9] (Capability Maturity Model for Software) by the organizations promoted the creation of similar models to address other areas not directly related with software development. Considering such aspect, many other models have arisen to support production systems, subcontracting areas, etc. But, all of these models were not created in order to facilitate integration among them, generating problems with their simultaneous implementation in an organization.

This fact has revealed the need of creating an integrated model, aiming a uniform view, besides the elimination of existing redundancies among the various maturity models. We can say that the CMMI is a result of a great integration work, and that it was elaborated to allow a convergence of the main existing maturity models. The CMMI structure also allows integration of new areas, which reinforces its integration capacity.

The CMMI SE/SW (Capability Maturity Model for Systems and Software Engineering) model V1.1 [5] consists of 22 Process Areas. A Process Area is a group of related practices that, when accomplished together, means that a set of important objectives were achieved, obtaining a significant improvement in such area.

All the CMMI Process Areas are common to the stage representation and the continuous representation. In the stage representation, the Process Areas are organized through maturity levels. Considering one level, all of its Process Areas are in the same maturity level. In the continuous representation, the maturity of a Process Area is called capability level and each Process Area can be in any of the six capability levels existents, independently of any other Process Area.

Thus, the name "maturity level" refers to a pre-defined group of Process Areas, which are in the same maturity level, whereas "capability level" refers only to an individual Process Area.

The continuous representation allows that one organization can choose the more adequate improvement sequence to its business goals, making possible a reduction of the risk areas.

The stage representation also offers a series of improvements, starting from basic management practices and going through a predefined plan of successive levels where each level is the basis for the next one.

To completely satisfy a Process Area, both generic and specific goals must be accomplished. Specific goals are applied to a Process Area and refer to single characteristics, which describe what has to be done to satisfy a Process Area.

The specific goals are supported by specific practices which are activities considered important to achieve a specific goal. The specific practices describe the activities, which must be accomplished in order to reach a specific goal of a Process Area.

Generic goals are called "generic" because a single goal can appear in multiple Process Areas. Considering the staged representation, every Process Area has a single specific goal. Generic goals are supported by common practices.

The CMMI continuous representation allows one organization to keep its capacity on the improvement of a single Process Area, or on multiple specific Process Areas. Each Process Area has its own specific goals associated similarly to the staged representation. Each capability level (from 0 to 5) has a common goal and many common practices.

The staged representation does not have requirements for the first maturity level; whereas, in the continuous representation there are specific and generic goals to be accomplished in order to achieve capability level 1. This has increased the granularity of the capability (process maturity), in such way that the organizations show early progress. This can be important in organizations that are under pressure to present immediate results.

The 22 Process Areas are divided into four categories, according to figure 1. In the activity of selecting a Process Area or a single category, an organization can focus its improvement efforts in such area. Each one of the 22 Process Areas can be characterized individually by the CMMI as having a maturity level from 0 through 5, as follows:

Capability Level 0 - Incomplete
An incomplete process is a partially accomplished or a non-accomplished process, that is, at least one of the specific goals of the Process Area is not achieved.

Capability Level 1 – Executed
At this level, processes achieve the specific goals of the correspondent Process Area. The process supports the necessary work to generate the required products from the inputs, which are correctly identified during the process. The difference between an incomplete process and an executed process is that an executed process achieves all the specific goals of the Process Area.

Capability Level 2 – Managed
A managed process consists in an executed process (capacity level 1), which is also planned and executed, according to a plan, which embraces qualified people, adequate resources and appropriate participants. The process is monitored, controlled, revised and evaluated according to its process description adherence and it can be instantiated to a design, group or organizational function. The process management comprises the Process Area institutionalization and the accomplishment of other specific objectives defined for the process, such as cost, time schedule and quality goals.

Capability Level 3 – Defined
A defined process is a managed process (capacity level 2), which includes a group of default processes according to the organization objectives, its metrics, and other information on process improvement.

Capability Level 4 – Quantitatively Managed
A quantitatively managed process is a defined process (capacity level 3), which is controlled through the use of statistics and other quantitative techniques. The quantitative objectives of quality and process performance are established and used as a criterion in the process management. The quality and process performance are transformed into statistics expressions and managed through the process lifecycle.

Capability Level 5 – Optimized
An optimized process is a quantitatively managed process (capacity level 4), which is modified and adapted to achieve the business and relevant goals in a specific moment. An optimized process is focused on the continuous improvement of the process performance through the use of technological improvement and innovative technologies.

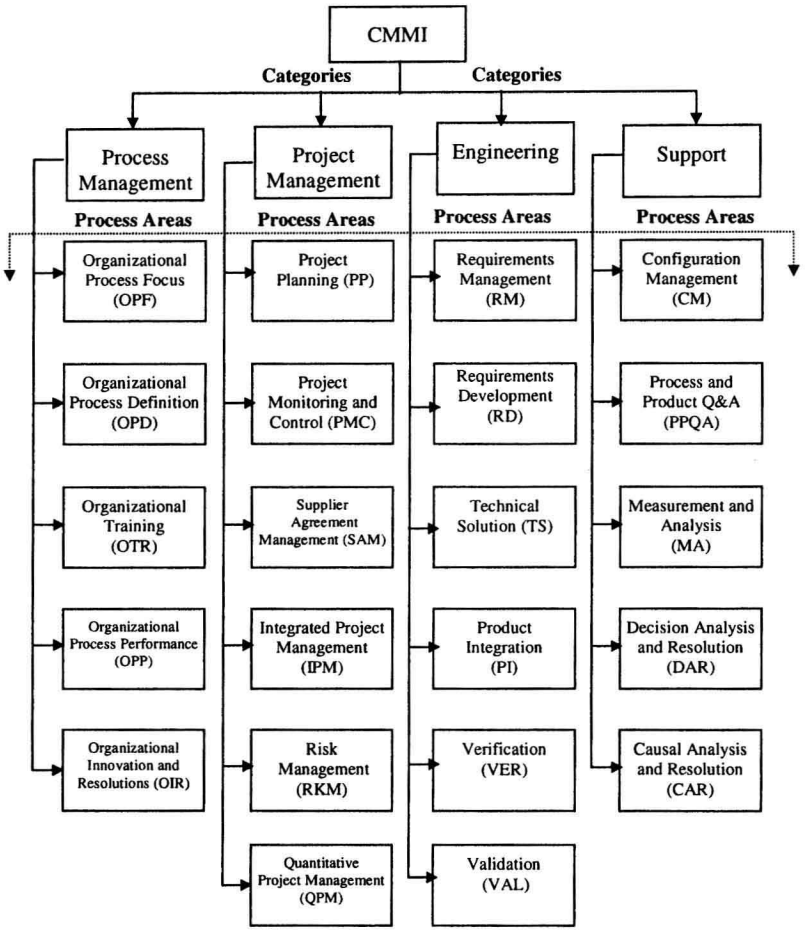

Fig. 1. CMMI Continuous Representation Process Areas

3 The CENELEC Standards

Since the first steps towards a single market of railway transport services in the European Union, it became evident the existence of different regulations in the safety issue.

The main reason for this situation can be explained by the fact that local national operators, which have all the responsibility for the systems operation inside their territories, perform the railway transport management of these countries. However, considering the increasingly integration of the European railway systems, the safety aspect should be considered in the most general ambit of the European Union [1].

At present, the railway industry is observing a process of developing appropriate safety standards that can control the new devices created by the technology development, seeking to ensure the adequate safety level for the systems. Railway