ASIGURAREA CALITĂȚII – QUALITY ASSURANCE

CUPRINS – CONTENTS

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XVIII, Issue 72, October-December 2012
Pages 2 - 11

Asigurarea survivabilității sistemelor informatice complexe

Costel CIUCHI, Laura IANCU, Gabriel PETRICĂ, Ioan BACIVAROV, Angelica BACIVAROV
EUROQUALROM Laboratory, ETTI, University POLITEHNICA of Bucharest, Romania
ciuchic@yahoo.com

Abstract
Defining essential capacities and fundamental quality attributes for systems are necessary to ensure optimum performance and to support strategies and objectives of an organization. Understanding the evolution of the quality characteristics and functionalities of the system in the presence of a fault can result from analyzing survivability – survival capacity of the system. Survivability can be defined as the set of technical and procedural measures taken to minimize the impact effect of an incident. Survivability has as fundamental purpose identifying the real costs of backup resources needed for restoration mechanisms to be added to a system to maintain services at a high level of performance. Survivability study of information systems, especially for Web applications, is a less explored domain in the literature. This article describes the SNA (Survivable Network Analysis) method in the context of Web applications developed on a 3-tier architecture through systematic evaluation of the proposed survival properties.

Keywords: survivability, security, strategy, SNA, decision, infrastructure.

References:

[1] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. A. Longstaff and N. R. Mead, „An Approach to Survivable Systems“, Technical Report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, 1999.
[2] R. J. Ellison, D. A. Fisher, R., C. Linger, H. F. Lipson, T. A. Longstaff and N. R. Mead, „Survivability: Protecting Your Critical Systems“, CERT Coordination Center Software Engineering Institute, IEEE Internet Computing, pp. 55-63, 1999.
[3] Y. Liu and K. S. Trivedi, „A general framework for network survivability quantification“, 12th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems together with 3rd Polish-German Teletraffic Symposium (MMB & PGTS 2004), VDE Verlag, 2004, pp. 369-378.
[4] R. J. Ellison, R. C. Linger, H. F. Lipson, N. R. Mead and A. Moore, „Foundations for Survivable Systems Engineering“, Technical Report, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, 2001.
[5] SURVIAC – DoD Survivability / Vulnerability Information Analysis Center, www.bahdayton.com/surviac.
[6] COM (2009) 149., COMUNICARE A COMISIEI CăTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ŞI SOCIAL EUROPEAN ŞI COMITETUL REGIUNILOR privind protecția infrastructurilor critice de informație „Protejarea Europei de atacuri cibernetice și

perturbaţii de amploare: ameliorarea gradului de pregătire, a securităţii şi a rezilienţei“, Bruxelles, 30.3.2009.
[7] Rezoluţia Consiliului din 18 decembrie 2009 privind o abordare europeană a securităţii reţelelor şi a informaţiilor bazată pe colaborare (2009/C 321/01).
[8] COM (2011) 163, COMUNICARE A COMISIEI CăTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ŞI SOCIAL EUROPEAN ŞI COMITETUL REGIUNILOR privind protecţia infrastructurilor critice de informaţie „Realizări şi etape următoare: către un context global de securitate cibernetică“, Bruxelles, 31.3.2011.
[9] R. J. Ellison et al., „Survivable Network Systems: An Emerging Discipline“, Tech. Report CMU/SEI-97-TR-013, Pittsburgh, Penn., Software Engineering Institute, Carnegie Mellon University, Nov. 1997 (revised May 1999).
[10] Bacivarov, I., and Mihai, I.C., „The Survivability Analysis of the Informational Systems“, Proceedings of the 11th International Conference of Quality and Reliability – CFF2008, Sinaia, 24-26 September, 2008, pp. 151-158, ISSN: 1842-3566.
[11] I. C. Mihai, I. Bacivarov, „Survivability Analysis Based on Attack Models“, Proceedings of the XIIIth International Conference of Quality and Reliability – CFF2012, Neptun, 5-7 septembrie, 2012, pp. 200-206, ISSN: 1842-3566.
[12] A. Avizienis, J.-C. Laprie and B. Randell, „Fundamental concepts of computer system dependability“, IARP/IEEE Workshops on Robot Dependability: Technological Challenge of Dependable Robots in Human Environments, Seoul, Korea, May 2001.
[13] Y. Liu and K. S. Trivedi, „Survivability Quantification: The Analytical Modeling Approach“, Int. Journal of Performability Engineering 2 No. 1 (2006): 29-44.
[14] C. Warren Axelrod, „The Dynamics of Privacy Risk“, Information Systems Control Journal, Vol. 3, 2004.
[15] http://msdn.microsoft.com/en-us/library/windows/desktop/ms685068(v=vs.85).aspx.S52
[16] Gary P. Schneider, „Electronic Commerce“, Third Annual Edition, Thomson Learning, 2002.
[17] http://msdn.microsoft.com/en-us/library/ee658117.aspx.
[18] R. Kazman, M. Klein, M. Barbacci, T. Longstaff, H. Lipson and S., J. Carriere, „The Architecture Tradeoff Analysis Method“, Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, IEEE Computer Society, 1998.
[19] Nancy R. Mead, Robert J. Ellison, Richard C. Linger, Thomas Longstaff, John McHugh, „Survivable Network Analysis Method“, CMU/SEI-2000-TR-013, ESC-TR-2000-013, September 2000.
[20] R. J. Ellison, R. C. Linger, T. Longstaff, N. R. Mead, „A Case Study in Survivable Network System Analysis“, Technical Report CMU/SEI-98-TR-014 ESC-TR-98-014, September 1998.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XVIII, Issue 72, October-December 2012
Pages 12 - 18

Defectarea componentelor electronice, fiabilitatea sistemului și ingineria de investigație

Titu-Marius I. BĂJENESCU[1], Marius BÂZU[2]
[1] C. F. C., La Conversion, Switzerland; [2] National Institute for Research and Development in Microtechnologies, IMT-Bucharest, Romania
tmbajenesco@bluewin.ch

Abstract
After a short introduction, the paper presents the problems concerning the reliable systems with non-reliable components, failure mechanisms and reliability problems, failure analysis, root causes, and localization of structural defect, packaging and globally competitive education.

Keywords: reliability, forensic engineering, failure analysis, failure mechanisms, physics-of-failure, packaging.

References:

[1] https://portail.telecom-retagne.eu/publi/public/download. jsp?id_publication=8696.
[2] Muratet, S., Conception, caractérisation et modélisation: Fiabilité prédictive de MEMS à actionnement électrothermique, Thèse de doctorat, Institut National des Sciences Appliquées de Toulouse, 24.11.2005.
[3] Palego, C., Composants MEMS RF pour les têtes de réception RF reconfigurables, Thèse de doctorat, Faculté des sciences et techniques de Limoges, 19 janvier 2006.
[4] de Nardi, C., Techniques d'analyse de défaillance de circuits intégrés appliquées au descrambling et à la lecture de données sur des composants mémoires non volatiles, Institut National des Sciences Appliquées, 25 mai 2009.
[5] Pareaud, Th., J.-C. Fabre et M.-O. Kilijian, „Conception orientée composant de mécanismes de tolérance aux fautes en vue de leur application en ligne", RenPar'18/SympA'2008/CFSE'6, Fribourg, 11 au 13 février 2008.
[6] Stanisavljevic, M., On the Dependability of Nanoscale Circuits and Systems: Methodologies and Circuit Architectures, Thèse de doctorat no. 4352(2009), Ecole Polytechnique Fédérale de Lausanne (EPFL), Suisse.
[7] http://www.cnrs.fr/comitenational/doc/rapport/2010/08_conj_2010.pdf.
[8] Evtodiev, I., Stări de impurități și defecte în materiale semiconductoare stratificate GaSe și InSe, Teză de doctor habilitat în științe fizico-matematice, Universitatea tehnică a Republicii Moldova, Chișinău, 17.9.2010, http://www.cnaa.md/files/theses/2010/16582/igor_evtodiev_thesis.pdf.
[9] Băjenescu, T.-M. I., M. Bâzu, Component Reliability for Electronic Systems, Boston and London, Artech House, 2009.
[10] Dennies, D. P., „The Organization of a Failure Investigation," Journal of Failure Analysis and Prevention, vol. 3, nr 2, June 2003.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XVIII, Issue 72, October-December 2012
Pages 12 - 18

[11] Venkataraman, S., „Diagnosis Meets Physical Failure Analysis: What is Needed to Succeed?," Proceedings of IEEE ITC International Test Conference 2004, p. 1442.
[12] Henderson, C. L., „Advanced to Failure and Yield Analysis," Overview of a 2 days course organized by Semitracks Inc., www.semitracks.com/courses/fa-course.htm
[13] Foucard, G., Taux d'erreurs dues aux radiations pour des applications implémentées dans des FPGAs à base de mémoire SRAM : prédictions versus mesures, Thèse de doctorat, Université de Grenoble, 2010-06-11.
[14] Gauthier, F., „La maintenabilité, une étude qui peut rapporter gros," Mesures, Février 2002, pp. 31-34.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XVIII, Issue 72, October-December 2012
Pages 19 - 25

The Use of Expert Systems in Evaluating the Quality of Universities Websites

Traian-Lucian MILITARU[1], George SUCIU[2], Gyorgy TODORAN[3]

[1] Quality Depart, University Politehnica of Bucharest, Romania; [2] 3CPS, University Politehnica of Bucharest, Romania; [3] EUROQUALROM-ETTI, University Politehnica of Bucharest, Romania
gelmosro@yahoo.com

Abstract
This paper proposes an expert system which can be used to evaluate the quality of websites own by some representative universities from Romania. The proposed expert system is using the Web Quality Assessment Method (WebQEM) developed between 1998-2000 by a group of researchers from the National University of La Pampa led by Luis Olsina and it was built using CLIPS expert system generator. CLIPS is a productive development and delivery expert system tool which provides a complete environment for the construction of rule based expert systems. In the first part of this paper, the WebQEM and CLIPS (C Language Integrated Production System) expert system generator are presented showing the advantage of using an expert system for this task. In the second part, a case study about the evaluation of websites owned by some representative universities in Romania is presented. The final conclusion of the experiment was that an expert system can successfully replace a human expert for the proposed task.

References:

[1] U.-D. Ehlers (Editor) and J. M. Pawlowski (Editor), „Handbook on Quality and Standardisation in E-Learning“, Springer, 2006, pp. 49-57.
[2] A. Balog, „Calitatea sistemelor interactive“, MatrixRom, 2004, pp. 93-94.
[3] J.J. Dujmovic, „A Method for Evaluation and Selection of Complex Hardware and Software Systems“, Resource Management and Performance Evaluation of Enterprise CS. CMG 96 Proceedings, The 22nd Int´l Conference for the, Vol. 1, pp.368-378.
[4] L. Olsina and G. Rossi, „A Quantitative Method for Quality Evaluation of Web Sites and Applications“, IEE Multimedia Magazine, October 2002, pp20-29.
[5] J. Peter, „Introduction to Expert Systems“, 3th Edition, Addison Wesley, pp. 2.
[6] CORPORATE JTEC Panel, „Knowledge-based systems in Japan“, Communications of the ACM Volume 37 Issue 1, Jan. 1994, pp. 17-20.
[7] E. Feigenbaum, E. Rich, G. Wiederhold and M. Harrison, „Advanced Software Applications in Japan“, 1st Edition, William Andrew, Jan. 1995, pp. 7.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XVIII, Issue 72, October-December 2012
Pages 26 - 28

A Reliability Management Technique for Autonomous Robots

Virgil L.M. ILIAN, Ioan C. BACIVAROV
EUROQUALROM –ETTI, University „Politehnica“ of Bucharest, Romania
bacivaro@euroqual.pub.ro

Abstract
Fault tree analysis has been used for decades in aeronautics, automotive, nuclear power, chemical processing industries, but it has seen limited use in mobile systems. The automotive industry has used the technique successfully but not dynamically. I propose the use of fault tree analysis as a dynamic technique that can allow an autonomous robot to properly evaluate its situation in the case of a fault. The utilization of fault tree analysis is a top down analysis technique that refers to aposteriori evaluations of undesired effects regarding the functioning of a system. This paper deals with the use of fault trees specifically constructed for each functional assembly/subassembly of an autonomous robot. These trees are stored in the system and subsequently used as a pattern for the automatic analysis of defects, faulty components and the probable causes of these faults. The results of these analyses are then used to evaluate the functioning capacity of the robot and (if possible) to attempt corrective actions in order to ensure continued functioning and mission completion. While the use of fault trees implies a large volume of work related to modelling the fault trees of each component of the robot, the autonomy the robot gains represents a major improvement on previous reliability management techniques. The system also permits the use of fault trees provided by manufacturers for their components with minimal adaptation. Furthermore, if the several robot models use the same components they can share the fault trees for those specific components by simply copying them reducing the volume of work even more. This makes the technique versatile in the long run allowing extremely complex robots to manage their own faults.

Keywords: Reliability, Faults, Robots, Autonomous Robots, Leaky Integrators.

References:

[1] C. Ericson, „Fault Tree Analysis – A History“, in The 17-th International System Safety Conference, 1999, pp. 1-9.
[2] W. E. Veseley, F. F. Goldberg, N. H. Roberts, and D. F. Heast, Fault Tree Handbook NUREG-0492. 1981, pp. 1-209.
[3] M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, Fault Tree Handbook with Aerospace Applications Fault Tree Handbook with Aerospace Applications. 2002.
[4] xxx „Military Electronic Reliability Design Handbook“, 1998.
[5] SR EN 61025 Fault tree analysis (FTA). 2007.
[6] V. L. M. Ilian, „Issues on reliability and operational safety of autonomous robots“, Research Report, UPB, 2012 .
[7] V. L. M. Ilian and I. C. Bacivarov, „Reliability and Safety Issues of Telepresence and TeleoperatedRobots“, in The 12-th International Conference on Quality and Dependability CCF2010, 2010, pp. 124-128.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XVIII, Issue 72, October-December 2012
Pages 26 - 28

[8] V. L. M. Ilian, „State of the art in robotics research“, Research Report, UPB, 2011.
[9] V. L. M. Ilian and I. C. Bacivarov, „Using leaky integrators in the administration of faults in an autonomous robot“, in The 13-th International Conference on Quality and Dependability CCF2012, 2012.
[10] I.Bacivarov, V. Catuneanu, „Fiabilitatea sistemelor de telecomunicatii“, Editura Militara, Bucuresti,1995.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XVIII, Issue 72, October-December 2012
Pages 29 - 32

Administration of Faults in an Autonomous Robot Using Leaky Integrators

Virgil L.M. ILIAN, Ioan C. BACIVAROV
EUROQUALROM –ETTI, University „Politehnica“ of Bucharest, Romania
cygnusgil@yahoo.com

Abstract
Autonomous robots are required by nature to have a large amount of reactive systems that are able to provide a time dependant response. This means the already limited resources available in autonomous robots have to accommodate a large number of time dependant decisional algorithms. Because of these limitations leaky integrators can fill the role quite well. They are lightweight in terms of computational power, easy to implement and easy to tune depending on the application. Since its discovery it has been used in electronics, mechanics and hydraulics. It has fit in particularly well in neural net models too successfully modelling a series of organic processes from neuroscience. Commonly used in reactive (bumper sensor based) navigation in autonomous robots leaky integrators can fill other roles too. In this paper we propose the use of leaky integrators as administrators of the warning flags sent by the defect detection system. In our case the defect detection system is a monitor that records and analyses the signals received from the robot sensors. A learned statistical model is used to evaluate the data (Ilian 2012) and highlight possible faults by triggering warning flags. The warning flags are then accumulated in a leaky integrator. If the trigger condition of the leaky integrator is reached it will in turn trigger a fault tree and a series of other systems to confirm and manage the fault (Ilian 2012). The implementation has proven to be robust and lightweight delivering results comparable to more complicated and computationally intensive event management systems. Favouring leaky integrators allows the redistribution of the limited computational resources of an autonomous robot to other processes that require them.

Keywords: Reliability, Faults, Robots, Autonomous Robots, Leaky Integrators.

References:

[1] C. Eliasmith and C. Anderson, Neural Engineering Computation, Representation, and Dynamics in Neurobiological Systems. 2003.
[2] „Bio-microelectronic informa tion processing device consisting of natural neurons on a cmos microsystem“, in Proc. Transducers 2007, Lyon, June 2007, 2007, no. June, pp. 1223-1226.
[3] K.-ho Lee, J. O. Lee, S. Choi, J.-bo Yoon, and G.-hyeong Cho, „Biosensors and Bioelectronics A CMOS label-free DNA sensor using electrostatic induction of molecular charges“, Biosensors and Bioelectronics, vol. 31, no. 1, pp. 343-348, 2012.
[4] H. Jaeger, „A tutorial on training recurrent neural networks , covering BPPT , RTRL , EKF and the ‘ echo state network ’ approach“, vol. 2002, pp. 1-46, 2008.
[5] H. Jaeger and M. Luko, „Optimization and applications of echo state networks with leaky-integrator neurons“, Neural Networks, vol. 20, pp. 335-352, 2007.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XVIII, Issue 72, October-December 2012
Pages 29 - 32

[6] R. W. Budelli, E. Soto, and O. Macadar, „Biological Cybernetics A Spike Generator Mechanism Model Simulates Utricular Afferents Response to Sinusoidal Vibrations“, Biological Cybernetics, 1986.
[7] V. L. M. Ilian and I. C. Bacivarov, „Fault tree analysis as a reliability management technique in autonomous robots“, in The 13-th International Conference on Quality and Dependability CCF2012, 2012.