SOCIETY
ROMANIAN SRAC FOR
QUALITY ASSURANCE

ASIGURAREA CALITĂȚII

QUALITY ASSURANCE

Ianuarie - Martie 2016 Volumul XXII Nr. 85

ASIGURAREA CALITĂȚII – QUALITY ASSURANCE

CUPRINS – CONTENTS

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XXII, Issue 85, January-March 2016
Pages 2-7

Quality Management in Media Corporations: New Requirements and Benefits

David Balme
Challenge Optimum SA, Geneve, Switzerland
david.balme@optimum.ch

Abstract
Media corporations, unlike any other company, have to satisfy two kinds of customers with potentially contradictory expectations : audience/readership and advertisers. Some of them even have to satisfy governmental expectations and/or requirements which add another layer of complexity in the production of contents. Those of them which aim at providing news to the general public are constantly threatened by biased editorial production due to the number and complexity of interactions with their stakeholders. Some key aspects of topicality necessary to forge public opinion may be simply hidden for untold reasons. Consequently, in order to help media corporations achieve editorial independence while serving the public interest, media professionals from all over the world have brought together their management know-how in a set of duly selected media specific requirements gathered in the so called ISAS MEDIA9001 standard, entirely based on ISO 9001. These requirements stand for the current best management practices so as to not only produce high quality news but also ensure long term sustainability of the media while aiming at serving the public interest.

Keywords: media management, newsroom, editorial independence, public interest, freedom of expression, censorship, quality management, risk, stakeholders, ISO 9001, ISAS MEDIA 9001

References:

[1] [BAL2015] ISO 9001:2015 : a key lever to take up the challenges of deregulated markets, change of consumption habits and make the best use of technological breakthroughs, Quality Assurance, September 2015.
[2] [BOE2014] Statistical Summary of Commercial Jet Airplane Accidents, Worldwide operations 1959-2013. Aviation Safety, Boeing Commercial Airplanes, August 2014.
[3] [CLICK2015] Click-N-Manage software, www.Click-N-Manage.com.
[4] [EDEL2016] Edelman Trust Barometer, http://www.edelman.com/insights/intellectual-property/2016-edelman-trust-barometer/.
[5] [GRI2012] Global Reporting Initiative sector guidance for the media industry (media Supplement), https://www.globalreporting.org/standards/sector-guidance/sector-guidance/media/Pages/default.aspx.
[6] [ISAS2016] ISAS MEDIA9001:2016 – A quality management standard dedicated to media industries (radio, TV, print media, Internet), http://www.media-society.org/en/isas-BCP-9001-standard.
[7] [ISAS2010] ISAS BCP9001:2010 – A quality management standard dedicated to media industries (radio, TV, print media, Internet), http://www.media-society.org/en/isas-BCP-9001-standard.
[8] [ISO9001] ISO survey 2014, http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2014.
[9] [MED2014] Newspapers Turning Ideas into Dollars, Four Revenue Success Stories.

[10] Pew Research Center's Project for Excellence in Journalism, 2013, www.journalism.org.
[11] [RWB2015] Reporters Without Borders World Press Freedom Index, 2015, http://index.rsf.org/#!/.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XXII, Issue 85, January-March 2016
Pages 8-10

Make Safer Products by Standardization the Risks

Steli Loznen
Israel Testing Laboratories Ltd., Israel
sloznen@ieee.org

Abstract
Increasing complexity of modern equipment and the systemic failures, often elude traditional testing and assessment. It is necessary to know how well particular equipment performs in relieving certain conditions, and what characteristics are associated with better and worse performance. Because it is impractical to expect absolute safety in the use of equipment the user must know how the equipment fails and why. Generally it is accepted that no system can be completely fail-safe and any associated risk should be reduced to a level which is as low as reasonably practicable. This is the new approach on Product Safety assessment based on the implementation of Risk Management. The Risk Management has become a key business process as an emerging philosophy across the industry. The standardization can play a major role in spreading this new culture. One of the potential standardization areas is represented by consideration of all the possible hazards and specifies the acceptable risk for each. The intent of the paper is to present proposed criteria in order to assist the standards developers to include in the product safety standards enough elements which will allow the users of standards to establish the acceptable levels of the risks.

Keywords: Standardization, Risk, Safety, Product Safety, Risk Management

References:

[1] ISO/IEC Guide 51:2014, “Safety aspects – Guidelines for their inclusion in standards”.
[2] ISO/IEC Guide 73:2002, “Risk management- Vocabulary – Guidelines for use in standards”, ILAC P-10:2002, Traceability of Measurement Results.
[3] IEC/ACOS/387/DC:2005, “ISO TMB/WG – Risk management – Guidelines for Principles and Implementation of Risk Management”.
[4] Medical Devices – Risk management Part 1: Application of risk analysis; Second Edition, ISO/IEC 14971-1 (Geneva: International Electrotechnical Commission, 2007).
[5] S. Loznen, “Product-Safety Requirements for Medical Electrical Equipment”, Compliance Engineering Vol.XII, No. 3(1995): 17-30.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XXII, Issue 85, January-March 2016
Pages 11-17

Security in Internet of Things: Mitigating the Top Vulnerabilities

Radu Boncea, Ioan C. Bacivarov
University Politehnica of Bucharest, Faculty of Electronics, Telecommunications and Information Technology, Romania
radu@rotld.ro

Abstract
With over 6 billion devices connected and transitioning from Do It Yourself to an enterprise model, Internet of Things (IoT) has to address several key challenges, among which the security and privacy have been identified as crucial. In the first part of the paper, the main problems regarding Internet of Things are presented. The top vulnerabilities of IoT – by their technical and business impact – are identified and mitigation measures are proposed in the second part of the paper . Finally, several European projects that have in their scope the security and the privacy of IoT and map their solutions to IoT vulnerabilities are analyzed.

Keywords: Internet of Things, IoT, Security, Privacy, Protocols, Architecture, vulnerabilities, Cloud Computing, Challenge, Future Internet, Internet of Everything

References:

[1] Balani, Naveen. Enterprise IoT: A Definitive Handbook. [ed.] Rajeev Hathi. ISBN 1518790860.
[2] Acatech – NATIONAL ACADEMY OF SCIENCE AND ENGINEERING. [Online] April 2013. [Cited: February 5, 2016.] http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf.
[3] Vermesan, Ovidiu and Friess, Peter, [ed.]. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. s.l. : River Publishers. ISBN: 978-87-92982-73-5.
[4] IERC – EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS. IoT Governance, Privacy and Security Issues. 2015. White Paper.
[5] Kelly, John E. Computing, cognition and the future of knowing. [Online] [Cited: February 6, 2016.] http://www.research.ibm.com/software/IBMResearch/multimedia/Computing_Cognition_WhitePaper.pdf.
[6] daCosta, Francis and Henderson, Byron. Rethinking the Internet of Things. 1st Edition. s.l. : Apress, 2013. ISBN: 978-1-4302-5740-0.
[7] IoT-A EU Project. Deliverable D1.5 – Final architectural reference model for the IoT v3.0. [Online] May 2013. [Cited: February 6, 2016.] http://www.iot-a.eu/public/public-documents/d1.5/at_download/file.
[8] Open Web Application Security Project (OWASP). Internet of Things Top Ten. [Online] [Cited: February 6, 2016.] https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf.

[9] Varakliotis, Socrates, Kirstein, Peter T. and Deiana, Giulia. The Use of Handle to Aid IoT Security. 2015.
[10] Federal Bureau of Investigation. INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME. [Online] September 2015. http://www.ic3.gov/media/2015/150910.aspx.
[11] Wikipedia. Metcalfe's law. [Online] https://en.wikipedia.org/wiki/Metcalfe%27s_law.
[12] National Institute of Standards and Technology. Electronic Authentication Guideline. June 2004. Special Publication 800-63.
[13] —. Guide to Storage Encryption Technologies for End User Devices. November 2007. Special Publication 800-111.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XXII, Issue 85, January-March 2016
Pages 18-26

On Implementation of Resilient Networks. A Case Study

Luminița Copaci, Angelica Bacivarov
EUROQUALROM, Faculty of Electronics, Telecommunications and Information Technology,
University "Politehnica" of Bucharest, Romania
lcopaci@yahoo.com

Abstract
The cost of failures within communication networks is significant. The communication networks – and the Internet in particular – are still vulnerable to malicious attacks, human mistakes such as misconfigurations, and a range of environmental challenges. In the first part of this paper the concept of resilience is defined and analyzed; its significance in different fields is comparatively analyzed. The main goal of this paper is to quantify via analytical models and simulation experiments the damage that a successful attacker can have on the performance of a communication network In particular, the paper is focused on studying resilience of ad hoc network. Consequently, the DoS attacks are analysed in order to assess the damage that difficult-to-detect attackers can cause. Our methodology is to study DoS resilience via a new and general class of protocol compliant denial-of-service attacks, which we refer to as JellyFish (JF). The JellyFish target closed-loop flows that are responsive to network conditions such as delay and loss. In addition to the JF attack, the Black Hole attack is studied, too.

Keywords: Communication networks, Resilience, Models, Simulation, Malicious attacks, DoS attacks, JellyFish, Black Hole

References:

[1] E. Hollnagel, D.D. Woods, and N Leveson. Reslience Engineering: Concepts and Precepts. Ashgate Publishing, 2006.
[2] S. Bohacek, J. Hespanha, J. Lee, C. Lim, and K. Obraczka. TCP-PR: TCP for persistent packet reordering, Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, May 2003.
[3] S. A. Begum, Techniques for resilience of Denial of service Attacks in Mobile Ad Hoc Networks, International Journal of Scientific & Engineering Research, Volume 3, Issue 3, March 2012.
[4] P. Smith, D. Hutchinson, M. Scholler, A. Fessi. M.Karaliopoulos, C. Lac, B. Plattner, Network Resilience: A Systematic Approach, IEEE Communications Magazine, pp. 88-97, July 2011.
[5] D.J Smith, Reliability, Maintainability and Risk, 7th ed., Elsevier, 2005.
[6] V. Gupta, S.V. Krishnamurthy, and M. Faloutsos. Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, Proceedings of MILCOM, 2002.
[7] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks, Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (MobiCom 2002), September 2002.
[8] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Ad Hoc Networks, 2003.

[9] Alin Copaci, Luminița Copaci, “Ensuring the Resilience against Denial of Service Attacks in Ad-hoc Networks”, Proceedings of the 11th IEEE International Conference in Quality and Dependability, Sinaia, sept 2008, pp. 179-186.
[10] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols, Proceedings ofWiSe 2003, September 2003.
[11] David B. Johnson and D. Maltz. The dynamic source routing protocol for mobile ad hoc networks (DSR), April 2003.
[12] V Kawadia and P. R. Kumar. Power control and clustering in ad hoc networks, Proceedings of IEEE Infocom, 2003.
[13] A. Kuzmanovic and E. Knightly. Low-Rate TCP-Targeted Denial of Service Attacks, Proceedings of ACM SIGCOMM 2003, Karlsruhe, Germany, August 2003.
[14] P. Michiardi and R. Molva. CORE: A Collaborative Reputation Mechanism To Enforce Node Cooperation In Mobile Ad Hoc Networks, Proceedings of The 6th IFIP Communications and Multimedia Security Conference, Portorosz, Slovenia, September 2002.
[15] P. Papadimitratos and Z. Haas. Secure data transmission in mobile ad hoc networks., Proceedings of WiSe, 2003.
[16] https://en.wikipedia.org/wiki/Denial-of-service_attack (accessed 10.01. 2015).
[17] F. Legendre, T. Hossmann, F. Sutton, B. Plattner, 30 Years of Wireless Ad Hoc Networking Research: What about Humanitarian and Disaster Relief Solutions? What are we still missing?, International Conference on Wireless Technologies for Humanitarian Relief (ACWR 11), 2011.
[18] M. Zhang, B. Karp, S. Floyd, and L. Peterson. RR-TCP: A reordering robust TCP with DSACK, Proceedings of IEEEICNP 2003, Atlanta, November 2003.
[19] I. Aad, J.-P. Hubaux and E. Knightly. Impact of Denial of Service Attacks on Ad Hoc Networks, in IEEE Transactions on Networking, 2008 .
[20] https://en.wikipedia.org/wiki/Resilience (accessed 20.04. 2014).

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XXII, Issue 85, January-March 2016
Pages 27-30

Systems on Chip (SoCs) and Reliability: Challenging Issues

Titu-Marius I. Băjenescu
C. F. C., La Conversion, Switzerland
tmbajenesco@bluewin.ch

Abstract
SoCs and microelectromechanical systems (MEMS) technologies could possibly enable in the next few years various space mission applications, medical imaging, remote sensing field, computer and IR vision, or other image processing applications. This paper is intended to inform non-SoC and non-MEMS technologists, researchers, and decision makers not only about the rich potential applications, but also too about some not yet solved important reliability key problems of reconfigurable SoCs. We still have limited knowledge on how such devices fail. Biggest challenge: cost effective, high volume packaging, self-healing SoCs.

Keywords: SoCs, MEMS, CMOS technology, embedded systems, reliability, failure mechanisms

References:

[1] Simunic, T., K. Mihic, and G. De Micheli, "Optimization of Reliability and Power Consumption in Systems on a Chip," Integrated Circuit and System Design, 2005, pp. 237-246.
[2] Băjenescu, T., M. Bâzu, Reliability of Electronic Components. A Practical Guide to Electronic Systems Manufacturing, Springer, Berlin and New York, 1999.
[3] Vassighi, A., "Heat and Power Management for High Performance Integrated Circuits," Doctor of Philosophy Thesis Presented to the University of Waterloo, Ontario, Canada, 2004.
[4] Bernauer, A., et al., "An Architecture for Runtime Evaluation of SoC Reliability," http://www.ti.uniuebingen.de/uploads/tx_timitarbeiter/bernauer-architecture-runtime-evaluation-soc-reliability-GIOC-06_01.pdf.
[5] Borkar, Shekhar, "Designing Reliable Systems From Unreliable Components: The Challenges of Transistor Variability and Degradation," IEEE Micro, 25(6), November/December 2005, pp. 10-16.
[6] Nourani, M., and A. R. Attarha, "Detecting Signal-Overshoots for Reliability Analysis in High-Speed System-on-Chips," IEEE Transactions on Reliability, Volume 51, Issue 4, Dec 2002, pp. 494-504.
[7] White Paper 2007, Virtuoso Ultrasim Full-Chip simulator, netlist-based electromigration voltage drop (EMIR) flow. http://www.cadence.com/rl/Resources/white_papers/emir_wp.pdf.
[8] ECSI Institute Workshop on Reconfigurable Systems-on-Chip, January 18, 2007, Hotel Ibis/Gares CDG Airport – Paris.
[9] Dallavalle, C., "Adaptive IDDQ: How to Set an IDDQ Limit for Any Device Under Test," Proceedings of the Eighth IEEE International On-Line Testing Workshop, 2002, p. 177.
[10] Chih-Wen Lu, Su Chauchin; Lee Chung Len, and Chen Jwu-E., "Is IDDQ Testing Not Applicable for Deep Submicron VLSI in Year 2011?," Proc. of the Ninth Asian Test Symposium, 2000. (ATS 2000), pp. 338-343.

Asigurarea Calităţii – Quality Assurance, ISSN 1224–5410
Vol. XXII, Issue 85, January-March 2016
Pages 27-30

[11] Ackerman, R., “Doing More With Less: A Recipe for Rapid IDDQ Development,” Proceedings of IEEE International Workshop on Current and Defect Based Testing, DBT, 2004, pp. 33-42.
[12] Masato Nakanishi, H. Masaki, H. Yotsuyanagi, M. Yukiya, “A BIC Sensor Capable of Adjusting IDDQ Limit in Tests,” 15th Asian Test Symposium, ATS ’06, 2006, November 2006, pp. 69-74.

15th International Conference "Quality and Dependability" CCF 2016

Participants at CCF 2014

The 15th edition of the International Conference "Quality and Dependability" - CCF 2016 will be organized in the conference halls of the Hotel Palace, Sinaia during the period 14-16 September 2016.

The conference is organized by the association Romanian Society for Quality Assurance, in cooperation with several national and international organizations in the field, under the scientific umbrella of the Romanian section of the Institute of Electrical and Electronic Engineers – IEEE.

Authors should take into account when preparing the CCF 2016 papers that can be addressed all sides - engineering, socio-technical, managerial, economic, and legal - and implications for quality and dependability (reliability, maintainability, availability, security, etc.). Consequently, the different points of view, including the polemic on engineering, management and certification of quality and dependability are welcomed for CCF in 2016; organizers take into consideration the organization of several debates and "round tables" on some controversial aspects of this interdisciplinary field of great interest.

The summaries, as well as the papers in extenso for CCF2016 must be sent via e-mail at the following addresses: CCF2016@srac.ro (Dr. eng. Dan G. Stoichitoiu - General Chairman of CCF 2016) and bacivaro@euroqual.pub.ro / ibacivarov@yahoo.com (Prof. univ. dr. eng. Ioan C. Bacivarov - Chairman of International Scientific Committee CCF 2016).
More information concerning CCF2016 is available at the following address:
http://www.srac.ro/en/evenimente.

ISSN 1224-5410