SOCIETY ROMANIAN FOR QUALITY ASSURANCE
SRAC

ASIGURAREA CALITĂȚII
QUALITY ASSURANCE

Aprilie - Iunie 2017 Volumul XXIII Nr. 90

ASIGURAREA CALITĂȚII – QUALITY ASSURANCE

CUPRINS – CONTENTS

ASIGURAREA CALITĂȚII – QUALITY ASSURANCE
Aprilie – Iunie 2017 Anul XXIII Numărul 90

Cybersecurity – A Global Priority

Ioan C. BACIVAROV*

EUROQUALROM – Faculty of Electronics, Telecommunications and Information Technology, University Politehnica of Bucharest, Romania

Information security and *cybercrime* represent an area of international importance because the integration of information technology and communications infrastructure in the Internet is accompanied by risks of intrusion and information compromise.

Nowadays Internet is the world's largest collection of networks that reaches government institutes, commercial enterprises, universities and research laboratories in all the countries. But along with easy access to information come new risks. The number of the attacks and the frauds on Internet is increasing fast.

Computer security seeks to thwart intruders through hardware and software devices that are independent of the domain of the application or system being protected. Software security methods like authentication, access control, cryptography, antivirus, firewalls and other mechanisms used in computer security are meant to protect an underlying application by Internet attacks. Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks [1].

The most recent *cybersecurity* alert was a global one, and has – once again – drawn attention to the global importance of this issue and the need to take effective actions to counter cyber-attacks.

Indeed, on May 2017, multiple companies and organizations around the world were hit by variations of a crypto-ransomware dubbed WannaCry / WannaCrypt / WanaCrypt0r / WCrypt / WCRY (generally called WannaCry for simplicity). The ransomware also acted as a worm and once it infects a system, it then self-propagates throughout the rest of the network. The ransomware campaign caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230,000 systems. Interestingly the attack was mounted on Friday 12th May 2017, just before the weekend, making it very difficult for companies and organisations to quickly react and resolve the crisis [1].

Due to the special actual importance of the ***cybersecurity*** problem, we decided to dedicate a special section of the international scientific journal "*Asigurarea Calitatii – Quality Assurance*" to this issue, including specialized cybercrime & cybersecurity articles written by field professionals.

In the first paper published in this section, **C. Pascariu**, **I.D. Barbu** and **I.C. Bacivarov** present an analysis on *WannaCry Ransomware*, related to the recent cybersecurity alert. The authors mention that with the advent of complex techniques, tactics and procedures used by the adversaries, Information Technology professionals focus their efforts on defending environments from advanced persistent threats and highly sophisticated attacks. WannaCry ransomware came in as a caveat in this context, a way of reminding the industry that efforts should be divided into addressing the various layers of the defense in depth model.

Their paper is intended to present this type of malware on the rise that affects users in both enterprise and personal space as well by encrypting user developed content and restricting access until ransom is paid. The main focus is on the description of the virus technical details concentrating on the phases of the

* Correspondence to Prof. **Ioan C. Bacivarov**, PhD, Director of the EUROQUALROM-ETTI-UPB laboratory, President of the Romanian Association for Information Security Assurance – RAISA, e-mail: **bacivaro@euroqual.pub.ro**, **ibacivarov@yahoo.com**.

cyber kill chain. Therefore, the authors perform an analysis of WannaCry ransomware from the delivery, infection, mitigation and detection perspectives.

The long-term goal of these efforts is to anticipate threats before turning into incidents and, consequently, decrease the impact. This research represents the starting point of a process of reducing the attack surface in the case of ransomware attacks. Needless to say, the first layer worth addressing is represented by the weakest chain in the information security link, the end user.

In the second paper of this section, **M. Best** (Germany) presents some general *data protection regulation* in the focus of data leakage. Two years ago, the new General Data Protection Regulation has been published by European Commission, that will turn into nation law of all EU member states on May 25th 2018. The new Regulation will replace the existing Directive and national data protection law. In many aspects, a lot of things have changed, and more obligations and responsibilities are to respect for data controllers. Sanctions according to the new Regulation are much higher than now. In the field of data leakage, there are also several interesting aspects to consider, which are discussed in this paper, too.

Finally, **I.C. Mihai** and **I.C. Bacivarov** present a study concerning the *cyber-attacks structure*. It is important to mention that the cyber-attacks experienced during the last period a great diversification and some of them can be classified as a *global epidemics*. There are many kind of *cyber-attacks* like malware: computer viruses, worms, trojans, adware, spyware, ransomware, rogueware, Distributed Denial of Service, e-mail and web based attacks. The authors examine and classify all these cyber-attacks using the intrusion model Kill Chain, defined by researchers from Lockheed Martin.

As a conclusion, the Romania, Europe and the entire world must learn from current events regarding cybercrime and be able to respond when the next crisis arrives.

At the same time, while organizations continue to purchase and deploy technical controls, not much has been done to focus on the *human side of cybersecurity* – so named *layer 8*[**].

Consequently, is of crucial importance for all the countries, professional organizations and companies to consolidate a powerful *cybersecurity culture*. From this point of view, the contribution of specialized technical magazines, such as our journal is, could be very important.

REFERENCES

[1] **I.C. Bacivarov**, Editorial, *International Journal of Information Security and Cybercrime - IJISC*, vol.1 (2012), no.1, pp. 6-7.
[2] **https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst** (accessed June 1st, 2017)
[3] **https://securityintelligence.com/building-a-cybersecurity-culture-around-layer-8** (accessed June 1st, 2017)

[**] The term layer 8 is often used pejoratively by some IT professionals to refer to employees' lack of awareness and a weak overall cybersecurity culture. Today, it is just as important to secure human assets — layer 8 — as it to secure layers 1 through 7 [3].

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXIII, Issue 90, April-June 2017
Pages 4-7

WannaCry Ransomware Analysis. 1 day, 150 countries, > 57k infected computers

Cristian PASCARIU, Ionuţ-Daniel BARBU, Ioan C. BACIVAROV
EUROQUALROM - ETTI, University "Politehnica" of Bucharest, Romania
crpascariu@gmail.com

Abstract
With the advent of complex techniques, tactics and procedures used by the adversaries, Information Technology Professionals focus their efforts on defending environments from advanced persistent threats and highly sophisticated attacks. WannaCry ransomware came in as a caveat in this context, a way of reminding the industry that efforts should be divided into addressing the various layers of the defense in depth model. This paper is intended to present this type of malware on the rise that affects users in both enterprise and personal space as well by encrypting user developed content and restricting access until ransom is paid. The main focus is on the description of the virus technical details concentrating on the phases of the cyber kill chain. Therefore, the authors perform an analysis of WannaCry ransomware from the delivery, infection, mitigation and detection perspectives. The long-term goal of these efforts is to anticipate threats before turning into incidents and, consequently, decrease the impact. This research represents the starting point of a process of reducing the attack surface in the case of ransomware attacks. Needless to say, the first layer worth addressing is represented by the weakest chain in the information security link, the end user.

Keywords: Cybersecurity, WannaCry, Ransomware, encryption, cyber kill chain, defense in depth, social engineering, MS17-010

References:

[1] Pascariu, C., Barbu, I.D. (2015). Ransomware – an Emerging Threat. International Journal of Information Security and Cybercrime, 4(2), 27-32. Retrieve from https://www.ijisc.com.
[2] https://www.us-cert.gov/ncas/alerts/TA17-132A.
[3] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.
[4] https://blog.malwarebytes.com/cybercrime/2017/05/wanacrypt0r-ransomware-hits-it-big-just-before-the-weekend/.
[5] https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/.
[6] https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europolsays/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html.
[7] https://blog.malwarebytes.com/cybercrime/2017/05/wannadecrypt-your-files/.
[8] https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXIII, Issue 90, April-June 2017
Pages 8-12

General Data Protection Regulation in the Focus of Data Leakage

Michael BEST
University "Politehnica" of Bucharest; Bensheim, Germany
mb@michael-best.de

Abstract
On May 25th 2016, the new General Data Protection Regulation has been published by European Commission, that will turn into nation law of all EU member states on May 25th 2018. The new Regulation will replace the existing Directive and national data protection law. In many aspects, a lot of things have changed, and more obligations and responsibilities are to respect for data controllers. Sanctions according to the new Regulation are much higher than now. In the field of data leakage, there are also aspects to consider, which will be discussed in this paper.

Keywords: Data protection, data leakage, regulations, GDPR, EU

References:

[1] GDPR: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
[2] Directive: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046.
[3] Charter of the fundamental Rights of the European Union: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[4] Paal, Pauly: GDPR, 2017, CH Beck (German).
[5] He lex loci solutionis is the Latin term for "law of the place where relevant performance occurs" in the conflict of laws.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXIII, Issue 90, April-June 2017
Pages 13-20

Cybersecurity. An Analysis on Cyber-Attacks Structure

Ioan-Cosmin MIHAI[1], Ioan C. BACIVAROV[2]
[1] Police Academy "Alexandru Ioan Cuza" University, Bucharest, Romania;
[2] EUROQUALROM - ETTI - University POLITEHNICA of Bucharest, Romania
cosmin.mihai@academiadepolitie.ro

Abstract
The recent cyber-attacks (May 2017) have increased the importance of the issue of cybersecurity at both national and global level. It is important to mention that the cyber-attacks experienced during the last period a great diversification and some of them can be classified as a global epidemics. There are many kind of cyber-attacks like malware: computer viruses, worms, trojans, adware, spyware, ransomware, rogueware, Distributed Denial of Service, e-mail and web based attacks. This paper examines and classifies all these cyber-attacks using the intrusion model Kill Chain, defined by researchers from Lockheed Martin.

Keywords: Computer, Security, Cybersecurity, Cyber-attack, Virus, Analyses, Intrusion model, Model Kill Chain

References:

[1] Gorman, S. and Barnes, J., "Cyber Combat: Act of War", 2011.
[2] Tidwell, T., Larson, R., Fitch, K. and Hale, J., "Modeling Internet Attacks", 2001.
[3] Cowan, C., Wagle, P., Pu, C., Beattie, S. and Walpole, J., "Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade", DARPA Information Survivability Conference and Expo (DISCEX), 2000.
[4] Hutchins, M. Eric., Clopperty, Michael J., and Amin, Rohan M., "Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", 2011.
[5] Majority Staff Report, "A Kill Chain Analysis of the 2013 Target Data Breach", 2014.
[6] ENISA Threat Landscape 2014, "Overview of Current and Emerging Cyber-Threats", 2014.
[7] Tulloch, M., Koch, J., and Haynes, Sandra, "Microsoft Encyclopedia of Security", Microsoft Press. 2003, p. 16.
[8] Preimesberger, C., "DDoS Attack Volume Escalates as New Methods Emerge", eWeek, 2014.
[9] Ramzan, Z., "Phishing attacks and countermeasures", Handbook of Information and Communication Security, Springer, 2010.
[10] Gragido, W., "Lions at the Watering Hole – The "VOHO" Affair", RSA Blog. EMC Corporation, 2012.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXIII, Issue 90, April-June 2017
Pages 21-25

The Impact of Human Factors on the Product Safety

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

Abstract
Human factors are all those things that enhance or improve human performance in the workplace. As a discipline, human factors are concerned with understanding interactions between people and other elements of complex systems. Human factors apply scientific knowledge and principles as well as lessons learned from previous incidents and operational experience to optimize human wellbeing, overall system performance and reliability. The discipline contributes to the design and evaluation of organizations, tasks, jobs and equipment, environments, products and systems. It focuses on the inherent characteristics, needs, abilities and limitations of people and the development of sustainable and safe working cultures. Situations where human error contributes to major incidents are often a consequence of inappropriate organizational arrangements or breakdowns in operational working practices. The main purpose of this paper is to bridge the gap between critical human tasks which are defined as those activities which people are expected to perform as barriers against the occurrence of an incident, or to prevent escalation in the event of an incident does occur and the principle of Product Safety. They include activities required to support or maintain physical and technological barriers.

Keywords: Safety, Ergonomics, Operator and Service, Human Factors

References:

[1] ANSI/AAMI HE 74, “Human factors design process for medical devices”, 2001.
[2] MIL-HDBK-759C, “Human engineering design guidelines”. Washington, D.C.: U.S. Department of Defense (DOD), 1998.
[3] ISO 18529, “Ergonomics – Ergonomics of human-system interaction – Human-centred lifecycle process descriptions”, Geneva, 2000.
[4] Ramsey, J., “Ergonomic factors in task analysis for consumer product safety”. Journal of Occupational Accidents 7, 1985, pp. 113-123.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXIII, Issue 90, April-June 2017
Pages 26-34

Challenges of Nanotechnologies and Some Reliability Aspects

Titu-Marius I. BĂJENESCU
La Conversion, Switzerland
tmbajenesco@bluewin.ch

Abstract
The paper take a fresh look at lessons learned from the last domain development. After a short introduction, is presented the advent of 3D Technology, the device shringing, carbon nanotubes, packaging and fabrication, critical dimensions, safety of environmental, health and safety (EHS), and the evaluation of reliability.

Keywords: nanotechnologies, reliability, Kaizen umbrella concept, Toyota way, lean production, innovation management

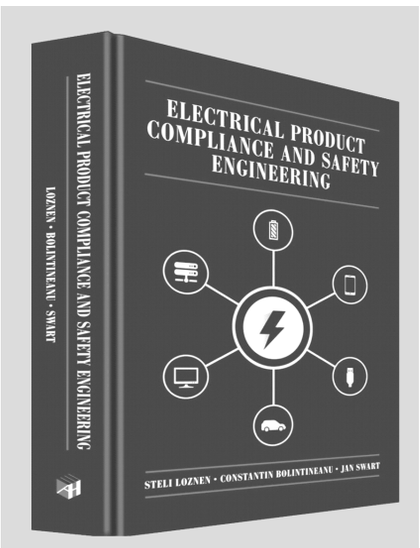
References:

[1] [AMA 02] Amakawa, S. K., Nakazato, and H. Mizuta, "A new approach to failure analysis and yield enhancement of very large integrated systems," Proceedings of 32th European Solid-State Device Research Conference, September 2002, Firenze, 147-150.
[2] [BAB 10] Băjenescu, T.I., and M. Bâzu, Component Reliability for Electronic Systems, Artech House, Boston and London, 2010.
[3] [BAJ] Băjenescu, T.I., "Micro Electro-Optical-Mechanical Systems (MEOMS), Microelectromechanical Systems (MEMS) and Reliability: Challenging Issues," Proceedings of 5th International Conference on Science of Electronic, Technologies of Information and Telecommunications, SETIT 2009, March 22-26, Tunisia.
[4] Băjenescu, T.I., "Nano-electronics and Reliability," EEA vol. 59 (2011), issue 4, 9-14.
[5] Băjenescu, T.I., "Challenges in Nanotechnologies and Manufacturing Processes," EEA vol. 60 (2012), issue 1, 75-79.
[6] Băjenescu, T.I., "Micro-comutatoare RF MEMS: fiabilitate, moduri şi mecanisme de defectare," Meridian ingineresc, Nr. 3(2013), 11-17.
[7] Băjenescu, T.I., "Grand Challenges and Relevant Failure Mechanisms of Nanoelectronic Devices," EEA Vol. 62 (2014), issue 2, 39-44.
[8] Băjenescu, T.I., Zuverlässigkeit elektronischer Bauelemente, Wiley VCH, Weinheim, 2017.
[9] [BAZ 09] Bâzu, M., et al., "Modern Procedures for Evaluating MEMS Reliability," Quality Assurance, Vol. XV, Nr. 57 (Jan.-March), 2009.
[10] [BHU 10] Bhushan, B., (editor), "Introduction to Nanotechnology", in Springer Handbook of Nanotechnology, pp. 1-13, Heidelberg and New York: Springer, 2010.
[11] [BOI 99] Boit, Ch., "Can failure analysis keep pace with IC technology development?", Proceedings of 7th IPFA '99, Singapore.
[12] [GER 09] Gerke, R.D., MEMS Packaging, Chapter 8, http://parts.jpl.nasa.gov/docs/JPL%20PUB%2099-1H.pdf.

[13] [KAN 06] Kang, Sung-Mo, “Nanoscience and nanotechnology: Status, potential and roadmap,” Proc. of 2006 Internat. Conf. on Communications, Circuits and Systems, Vol. 2, p. 17.
[14] [KJE 07] Kjelstrup-Hansen, J., “Integration of nanocomponents in microsystems,” 4th Nanoworkshop at SDU (University of Southern Denmark), March 8, 2007.
[15] [MAR 07] Martin, H., and T. Daim, “Technology roadmapping through intelligence analysis: nanotechnology,” Portland Internat. Center for Management of Engineering and Technology, 5-9 August 2007, 1613-1622.
[16] [MCC 08] McConachie, C.R.,“Practical issues in commercial and regulatory development of nanotechnology; the good, the bad and the ugly,” Proc. of 8th IEEE Conf. on Nanotechnology 2008, Nano ‘08, 870-873.
[17] [MUN 06] Munetoshi, F.M., M. Yasuhiro, M. Yasuhiko, Y. Fumiko, and F. Takashi, “Invisible failure analysis system by nano probing system,” Hitachi Hioron, Vol. 88 (2006). No. 3, 287-290.
[18] [MYH 08] Myhailenko, S., A., S. Luby, A. M. Fischer, F. A. Ponce, and C. Tracy, “SEM characterization of silicon nanostructures: Can we meet the challenge?” Scanning, Volume 30 Issue 4 (June 2008), 310-316.
[19] [ROC 01] Roco, M.C., “International strategy for nanotechnology research and development,” Journal of Nanoparticle Research, vol.3, (2001) 353–360.
[20] [SHU 02] Shuttleworth, D.M., A new failure mechanism by scanning electron microscope induced electrical breakdown of tungsten windows in integrated circuit processing, Master of Science Thesis, University of Florida, 2002. http://pearton.mse.ufl.edu/theses/DavidShuttleworth.pdf
[21] [TAN 01] Tanner, D.M., and M.T. Dugger, “Wear Mechanisms in a Reliability Methodology,” SPIE Proceedings, Vol. 4980, January 2001, 22-40.
[22] [TRM] Technology Roadmap for MEMS, http://www.mosti.gov.my/mosti/images/pdf/MEMS.pdf.
[23] [VOL 09] Voldman, S.H., ESD Failure Mechanisms and Models, Chapter 8, Chichester and New York: J. Wiley & Sons, 2009.

BOOK REVIEW

Steli Loznen, Constantin Bolintineanu, Jan Swart
Electrical Product Compliance and Safety Engineering



Artech House, 2017

ISBN 978-1-63081-011-5, 400 pages, $149

Electrical products are increasing in complexity and diversity, leading to an increase in product-related harms. Since electrical products are becoming more sophisticated, there are more complex aspects linked with the *Compliance* and *Safety*. It is unanimous accepted that the manufacturers around the world have responsibility to produce products that satisfy the safety expectations of society.

The growing field of Compliance and Safety, as a global function acts as a cross-functional discipline which has a direct impact on people's lives. The term 'safety' has many different connotations and it can be related to many different concepts such as occupational health and safety, road safety or product safety.

Majority accept that p*roducts safety issues* are important in customer and professional areas, engineering, management and other fields. This aspect is obvious due to the fact that products compliance and safety is now a global issue, because markets are global.

Publishing the book *Electrical Product Compliance and Safety Engineering*, ***Artech House***, a prestigious publisher located in London and Boston, intended to develop an attitude, an approach, and a concept for the professionals in the field.

Actually, a large amount of information related to Product Compliance and Safety can be found, but spread in many sources without a unitary presentation. *Electrical Product Compliance and Product Safety* it is the first book which put together the main information in the field, becoming a comprehensive resource designed to guide professionals in product compliance and safety in order to develop safer and profitable products.

The first goal of the book is to present the basics of *Product Compliance and Safety*, considering the key actions for implementing these issues. There is a second purpose, equally important: to promote the idea that on developing and manufacturing an electrical product need to have developed a *culture of compliance and safety*, to show the importance of this discipline in our days and the necessity to support their goals, as a discipline, in achieving a given level of Safety, as a key characteristic of any electrical product.

Even more important, this book is aimed to show to industry managers the reasons for taking into account the compliance and safety issues, even from the design phase and then during the whole life cycle of any electrical product. It was proved that the only way to promote compliance and safety requirements is top-down, starting from the manager and going down to every worker.

The content of the book, divided into sixteen chapters, was chosen to provide background on why need to know Compliance and Safety Engineering for Electrical Products and how to use the information provided.

Chapter 1 examines **Why Electrical Product Compliance and Safety** need, by referring to Product Compliance and Safety in 21st century, Electrical Product Safety Legislation and Liability, Designing for Safety and Safety Cost Estimation

Chapter 2 makes an introduction to **International Regulations and Global Market Access Regulations**, addressing the Regional regulations and how they differ, CE Marking, National Recognized Testing Laboratories (NRTL), IECEE CB Scheme, Product Certification Marks and the ISO Registration Process.

Chapter 3 addresses the **Products Safety Standards** and Standardization presenting what is a standard and his structure; what means the conformity to standards; which types of Products Safety standards exist and

which are their objectives, grouping in the final of the chapter the main Standards development organizations.

Chapter 4 covers the **Electrical Products Safety Philosophy** analyzing the concepts of Safety, Reliability, Product Safety, Perception of the Risk, Failure, Single Fault Safe, Redundancy, Safety Factors, concluding with the differences between Work Safety and Product Safety.

Chapter 5 introduces the **Methods for Failure Analysis**: FMEA, FTA, HAZOP, AEA and ETA.

Chapter 6 presents the **Risk Management for Product Safety**, by detailing the process: Identification of Hazards, Estimation of the Risk, Risk Evaluation and Risk Control. Dedicated sub-chapters are for Functional Safety and for Standards used for Risk Management.

Chapter 7 deals with the **Electrical Products Safety Concepts**: Means of Protection, Insulation Diagram; Safe Current and Voltages Limits; Leakage Currents, Spacing: Air Clearance and Creepage Distances, Grounding, Fire, Electrical, Mechanical Enclosures; Ratings; Type of Circuits, Normal Load and Abnormal operating conditions.

Chapter 8 is dedicated to **Selection of Components**: Semiconductors, Passive components, Temperature control devices; Motors, Fans, Thermoplastic materials, Terminal Blocks, Connectors, Internal Wiring

Chapter 9 examines the **Batteries**: secondary and primary, including the main applicable standards; a particular attention is paid to Battery Safety Design.

Chapter 10 addresses the **Power Sources** and the associated components: Power Supply Plugs, Connectors and Cord Sets, Fuses, Fuse holders, Power Entry Module, Switches, Varistor, Transformers and Power Supplies

Chapter 11 describes typical **Product Construction Requirements**: Enclosures, Circuit Separation, Grounding and Bonding, Resistance to Fire and Flame Rating, Interlocks, Moving Parts, Part subject to Pressure, Constructive aspects related to EMC. Information about Serviceability makes the object of a special sub-chapter

Chapter 12 looks at **Markings, Indicators and Accompanying Documents** describing the Internal and External marking, Safety labels, Marking of controls and instruments, Color of indicators. User's Manual and Installation Instructions, Safety instructions, cautions and warnings.

Chapter 13 addresses **Human Factors and Product Safety**, pointing in the followings: Operator and Service Personnel, Human Factors, Ergonomic Hazards.

Chapter 14 (the largest part of the book) is dedicated to **Testing for Compliance and Safety** and consists of: Kind of Product Basic Safety and EMC tests, Information typically required for Product Basic Safety and EMC testing, Work Safety in a Product Basic Safety and EMC testing laboratory, Equipment used on Product Basic Safety and EMC Testing, General testing conditions, Product Basic Safety Testing, EMC Testing and Software Testing.

Chapter 15 examines how **Manufacturing a Safe Electrical Product** by referring to: Responsibility of the Manufacturer, Supply chain, Manufacturability, Integration and Routine Tests (Production Line Testing)

Chapter 16 provides some inputs on the **Education and Training for Compliance and Product Safety Professionals** analyzing the Compliance and Product Safety Engineering in Senior Design Courses; Training Resources Development and the Professional Certification.

The **Glossary of Terms** and **Acronyms** included in the Appendix helps as a quick reference to deal with the issues at hand.

The authors have structured this book in an easy to read and follow fashion, from product design considerations, to manufacturing and prototyping, conformity assessment necessities and the sustaining engineering principles. Also, they have provided a logical and meaningful contribution to the overall process of facilitating the entry of safe products into the various global markets.

A strong point which recommends this book are the authors: **Steli Loznen**, **Constantin Bolintineanu** and Dr. **Jan Swart**, three well known specialists and experts in the field, with a long experience in the domain of Compliance and Safety, Standardization, Testing, International Regulations and Failure Analysis.

Electrical Product Compliance and Safety is an essential reference and text book that will prove of great importance for all professionals involved in the design, manufacturing, testing, servicing and marketing of electrical products, as well is intended also for instructors and students on electrical and electronics departments of Engineering Universities, by adding to the training syllabus an issue which was neglected until today.

Consequently, I highly recommend this book, which is among the best ones in its category.

Professor **Ioan C. BACIVAROV**, PhD
Director of EUROQUALROM – ETTI Laboratory
University "Politehnica" of Bucharest, Romania
Editor-in-Chief
"Asigurarea Calitatii – Quality Assurance"
Editor for Europe *"Quality Engineering"* (U.S.A.)